Chapter IX

Online Child Pornography and Exploitation

by Geoff Allard

I. Introduction

This chapter is intended to be used by line prosecutors rather than task force specialists who specialize in online child pornography and exploitation. It is designed to guide the prosecutor through the investigative and prosecutorial phases of online child exploitation cases and aims to simplify and explain the practical and technological concepts involved so that both the prosecutor, and ultimately the jury, can understand and appreciate the nature of these often complex and emotional cases.

II. Mental Preparation

The first thing a prosecutor should do when he or she receives a case involving child pornography is, to the extent possible, to prepare mentally. At the same time, the prosecutor must realize that there is no amount of mental preparation that can fully prepare a person emotionally for a first-time viewing of photographs of infant and child rape. Child pornography cases may exact a mental toll on police and prosecutors alike.

A. Keep in Mind the Importance of the Prosecutor's Mission

One thing that may help prosecutors prepare for the revolting crime they will be prosecuting, and the disturbing evidence they will be required to review, is to keep in mind the importance of their mission. They should remember that horrible sexual crimes are being visited upon children worldwide. One cannot overestimate the importance of a prosecutor's mission in prosecuting a child pornography or child exploitation case.

Prosecutors should also remember that in putting a suspect behind bars, they are not merely putting away someone who is harmlessly viewing taboo photos (whether out of curiosity or actual misguided sexual interest). The defendant is very possibly a current or aspiring child molester. Sexuality is the most fundamental aspect of human behavior. It only makes sense that if someone is sexually attracted to an eight-year-old child, he will act on that attraction if given the chance. By putting a consumer of child pornography behind bars, prosecutors are likely doing more than advancing the abstract good of diminishing the market for child pornography. More that likely, they are also preventing the victimization of an innocent and helpless child. This knowledge will not make looking at the evidence any more pleasant, but it might offer some small amount of comfort.

B. Remain Objective

Finally, while prosecuting a child-pornography or any child-exploitation case, it is vital that prosecutors balance their aggressive prosecution with objectivity. A prosecutor will almost certainly be revolted—not only by the evidence and by the contraband in the defendant's possession—but by the defendant himself. This is natural when confronting an individual who has chosen to make victims of society's most helpless members for his own sexual satisfaction. This reasonable reaction of disgust should **never** negatively affect the prosecutor's objectivity as to the strength of the evidence and case.

III. Practical Requirements

In addition to a strong stomach and a strong will to see that justice is done, prosecutors also need to have a good grasp of Internet and computer technology basics and a qualified, competent computer-forensics expert for a successful prosecution.

A. A Basic Understanding of the Internet, the Primary Medium for Pornography Transmission

First, prosecutors need a working knowledge of the Internet—they should know in basic terms what it is, and how Internet users access and interface with it. Moreover, prosecutors should have a working knowledge of computer operating systems, computer hardware, computer software, and forensic examination. These matters are discussed in some detail below.

B. A Credible Expert

Second, a credible and qualified computer-forensics expert is needed, who can not only examine the defendant's computer, but also translate the results into basic understandable English for jurors. Computers are very complex systems. In explaining how they work to the jurors, the expert must avoid using technical jargon that will confuse the jurors or put them to sleep.

This applies to prosecutors as well. It is their responsibility to package this information in a persuasive, yet completely user-friendly format for jurors. Since computer technology is highly technical, both the prosecutor and the forensic expert will need to resort to analogies, describing the computer processes using illustrations that are familiar to the average person. The sections to follow address what the computer forensics expert should be prepared to testify to and some sample questions for prosecutors to use when examining the computer-forensics expert.

IV. A Short History of Child Pornography

Child pornography cases were once rare, arising only when police came across private collections of magazine clippings, Polaroid photographs, and the occasional videotape or film. Obscenity law covered the legality of possessing such material, and the community had to decide whether the material lacked redeeming social or educational literary value.

In *New York v. Ferber*,[1] the United States Supreme Court did away with the "right" to possess and view images of sexually abused children, holding that the right of children to be protected from a lifetime of repeated exploitation through endless viewing of their abuse far outweighed the privacy

rights of the individuals who collected and viewed the images. Eventually, the California Legislature, through a series of amendments, adapted child exploitation laws to cover child pornography.

In California, lawmakers have moved at a snail's pace compared to the evolution of digital technology that allows a photo to go around the world in a matter of seconds: right click, left click, global distribution. An overview of current California law is given below.

V. Child Pornography—What It Is and What It Is Not

A. What Child Pornography Is

The term "child pornography" in fact does not appear once in California's lengthy and often confusing definition provided by Penal Code section 311.3. Put most simply, child pornography is any image or video of a real child under the age of 18 engaged in or simulating sexual conduct. Penal Code section 311.3 defines it as material that portrays sexual conduct, meaning any of the following:

1. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex or between humans and animals.

2. Penetration of the vagina or rectum by any object.

3. Masturbation for the purpose of sexual stimulation of the viewer.

4. Sadomasochistic abuse for the purpose of sexual stimulation of the viewer.

5. Exhibition of the genitals or the pubic or rectal area of any person for the purpose of sexual stimulation of the viewer.

6. Defecation or urination for the purpose of sexual stimulation of the viewer.

B. What Child Pornography Is Not

1. "Art"

The image in question must be of a real child. Anime,[2] drawings, and animations that depict the most offensive sexual crimes against children are widely traded. While these materials may be obscene, they are legal child pornography under current law. But this obscene "art" may still be useful evidence. For example, the defendant who claims that the photographs of his young niece naked in his backyard are merely the type of innocent pictures present in any normal family photo album, the presence of a few cartoons depicting the rape of a schoolgirl in the defendant's collection may show the requisite bad intent behind his possession of the photographs. Hopefully, the cases that warrant prosecution will include obvious examples of real child pornography, and not merely the kinds of pictures that, in another context, might appear to be harmless family photos.

2. "Innocent" nude photos of minors

Clearly, innocent photos of an unclothed child playing under a sprinkler or in the bath are not child pornography as their purpose is not to elicit a sexual response.

Furthermore, there is a genre sometimes referred to as "child erotica," which also does not conflict with the law. While the notion of using an image of a child to depict eroticism is distasteful to most people, it is not necessarily illegal under current law.

Nude photos are not child pornography unless the photographer obviously focused on the genital or anal area. Even a photograph of a topless six-year-old in a thong may not constitute child pornography.

C. A "Child Porn" Test—The *Kongs* Analysis

People v. Kongs focuses the analysis of whether or not an image is child pornography on the viewer's intent.[3] In making a determination, prosecutors should consider the content of the images as well as their context, and base their analysis on the following *Kongs* factors:

1. Whether the focal point is on the child's genitalia or pubic area.

2. Whether the setting is sexually suggestive (i.e., in a place or pose generally associated with sexual activity).

3. Whether the child is in an unnatural pose or in inappropriate attire, considering the age of the child.

4. Whether the child is fully or partially clothed, or nude.

5. Whether the child's conduct suggests sexual coyness or a willingness to engage in sexual activity.

6. Whether the conduct is intended or designed to elicit a sexual response in the viewer.

It should be noted that *Kongs* also held that not all of the factors must be present in order for an image to qualify as illegal child pornography. The *Kongs* court held that "a trier of fact need not find that all of the first five factors are present to conclude that there was a prohibited exhibition of the genitals or pubic or rectal area: the determination must be made based on the overall content of the visual depiction and the context of the child's conduct, taking into account the child's age."[4]

VI. How Do Prosecutors Get These Cases?

There are a number of specialized units whose main function is to prosecute child exploitation cases. But the scope of the problem is so great that these units cannot possibly handle every case that warrants prosecution. So the line deputy, possibly with little computer experience and no experience prosecuting sex crimes, should not be too surprised when a child pornography case lands on his or her desk. The following are ways in which prosecutors may receive child pornography cases.

A. Repair Shop Referral

It is common for an individual who has been using his computer to download and view illegal child pornography to have computer repairs performed without bothering to delete those files. But as explained more fully below, even if efforts to delete the contraband files have been made, the files often remain on the disk in part or in whole, due to the way computer operating systems delete files.

Computer repair facilities increasingly are calling law enforcement to report discovery of child pornography.

1. Search issues

When a computer technician goes through the files on a customer's computer, whatever his motivation might be—a legitimate inspection for the purposes of completing a diagnosis or repair, or pure nosiness—he is not violating the Fourth Amendment, which controls only the actions of government agents. Furthermore, law enforcement may observe or even replicate the search performed by the computer technician and may use observations to seize the computer and obtain a search warrant. But law enforcement may not search more expansively than the private actor did without first obtaining a search warrant.

While repair facilities should always be encouraged to do their civic duty and protect the good name of their business by reporting such discoveries to law enforcement, rewarding them in any way or giving them specific instructions for what to do in the event of future discoveries could be construed by courts as an action making them an "agent" of law enforcement. If the court found this to be the case, the court could extend Fourth Amendment protection over the customer at the repair shop in that particular instance.

Given forfeiture laws, search warrants are often obtained for a defendant's home and computer based on discovery. First, the defendant is given the repaired computer and charged accordingly. The search warrant is executed once the computer is back in the possession of the defendant. The search warrant reveals child pornography on the computer and law enforcement seizes the computer per Penal Code section 502.01(c).

Note: Do not allow a third party who searches a computer to become an agent of law enforcement.

2. Case law

a. *United States v. Jacobsen*[5]

The Supreme Court presented the framework that should guide agents seeking to uncover evidence because of a private search. According to *Jacobsen*, agents who learn of evidence via a private search can reenact the original private search without violating any reasonable expectation of privacy. What the agents cannot do without a warrant is "exceed the scope of the private search."[6]

b. ***United States v. Hall***[7]

During a central processing unit (CPU) repair/upgrade, a technician saw unusually named files and viewed three to five files (of 1,000 files total). The technician called a state trooper and described two or three images to the trooper. The trooper then had the technician copy several of the files onto a disk. The court held that evidence discovered by the technician constituted a private search and was admissible. Although the government conceded that the copying of files to disk was a warrantless search, the copied disk was never reviewed by law enforcement nor used as a basis for probable cause in the search warrant and, therefore, the warrant was valid.

c. ***United States v. Barth***[8]

A computer technician reviewing files on a hard drive became a government actor when he contacted an FBI agent for whom he worked as a confidential informant and was told to copy the pornographic files onto disks. The defendant had a reasonable expectation of privacy in his computer files, which continued while the technician had custody of the computer to perform repairs. The search violated the Fourth Amendment.

d. ***United States v. Grimes***[9]

The defendant's wife brought the defendant's computer into a repair shop and authorized a "cleaning" of the system. An employee followed the standard approach of looking at JPG files prior to deleting them and subsequently reported the discovery of child pornography to law enforcement. On its own, the repair shop copied images and gave them to law enforcement officers. The court found that the initial search was private and outside of the Fourth Amendment. It also found that pre-warrant viewing of the images by the FBI was still within the scope of the private search and that the defendant no longer possessed an expectation of privacy.

Penal Code section 11165.7, while still incorporating animal control officers as mandated reporters, does not include repair technicians.

B. Employer Referral

Most employers require employees to acknowledge, in writing, the management's right to search and monitor their computer activity for inappropriate material. Oftentimes, the user is obligated to acknowledge such a waiver by clicking a consent-to-search "banner" each time he logs into a company computer. If the employer finds child pornography on the suspect's work computer, the data is often preserved (in varying levels of forensic integrity), the suspect fired, and law enforcement contacted all in the same day.

1. Search issues

If an employer gives consent to search, the prosecutor should still obtain a search warrant to cover a possible withdrawal during forensic examination. Written documentation of the

employee's acknowledgment of company's computer policy and waiver of privacy rights should also be obtained.

2. Case law

a. *United States v. Simons*[10]

The defendant, an employee at CIA's Foreign Bureau of Information Services, did not have a reasonable expectation of privacy regarding his Internet use in light of his employer's written policy. Searches of his computer and office were found reasonable.

b. *Muick v. Glenayre Electronics*[11]

The defendant, an employee of an electronics company, did not have a reasonable expectation of privacy in a work-issued computer, where the computer was for use in the workplace and the employer could inspect the computer at any time. The fact that the employer seized the computer at the request of law enforcement did not make the employer an agent of the police where there was no agreement between the two and, in fact, the employer refused to relinquish the computer until forced to do so by warrant.

c. *United States v. Angevine*[12]

The defendant had no reasonable expectation of privacy in a work computer where an employer (university) reserved ownership and monitored use of computers, and thus no right to a *Franks* hearing.[13]

d. *United States v. Slanina*[14]

A government employer, who was also a law enforcement official, had the right to conduct a warrantless search of the employee's computer. Even though an employee's suspected misconduct is also a criminal offense, the search is reasonable if it remains, even in part, an investigation of workplace misconduct. Once searched by the employer, the FBI could conduct a more exhaustive warrantless search of the same computer.

Note: Here the court found that the defendant did have a reasonable expectation of privacy in his work computer because the computer was password protected and the employer had no policy for (1) preventing the storage of personal information on computer, or (2) monitoring computer usage.

e. *United States v. Wong*[15]

The defendant lacked standing to object to a warrantless search of a laptop used in prior employment because he failed to establish that he had a reasonable expectation of privacy in it.

f. ***United States v. Thorn***[16]

In light of the government agency's computer-use policy, the government employee had no legitimate expectation of privacy as to the use and contents of his office computer. Therefore, evidence found during a warrantless search of the computer was admissible in prosecution for possession of child pornography. The employee was fully aware of the policy that specifically barred certain unauthorized use of the agency's computers and provided that employees had no personal right of privacy with respect to their use of the computers, and that the agency had the right to access the computers to audit their employees' use.

g. ***People v. Jiang***[17]

Information intended for the defendant's attorney, contained in password-protected documents located a laptop issued by his employer, was protected by attorney-client privilege. The employer's computer-use policy was not specific enough to overcome the defendant's right of privacy.

C. E-mail Reporting from an Internet Service Provider

An Internet Service Provider (ISP) faces huge fines by the federal government for knowingly allowing child pornography to be used, stored, or transmitted on its network.[18] As a result, most ISPs have language in their Terms of Service (TOS) agreement warning customers that the ISP has the right to monitor the content of transmitted e-mail and online storage for inappropriate material, and that law enforcement will be notified if it is found.

If information is provided by the ISP pursuant to a TOS violation, a search warrant should be obtained to further search the suspect's computer.

D. Credit Card Billing Database Seizure

For example, while some Web sites have switched over to anonymous billing processes such as Pay-Pal or E-Gold, others still believe that by existing beyond the borders of the United States they are insulated from discovery or prosecution, and continue to allow the use of bank-issued credit cards such as Visa or MasterCard to facilitate their purchases. If these credit card databases are seized by United States or foreign authorities, the often-voluminous information contained in them can be a gold mine for investigators willing to take the time to parse out the information among the different state and federal jurisdictions and write the search warrants to search the suspects' homes and computers. Several operations, including Immigration and Customs Enforcement's "Operation Falcon" have succeeded in the arrest and prosecution of hundreds of individuals who were not only exploiting children online via their downloading of child pornography, but who were actively molesting children as well.

1. Search issues

Child pornography is a $20 billion a year business. And as any other purchase made online, payment for child pornography involves electronic transactions.

While certainly much child pornography has been and continues to be hosted on computers located in the United States, in recent years, many Web sites that sell "subscriptions" to child pornography have moved offshore to avoid prosecution. Most of these companies use third-party billing Web sites to handle credit card transactions. These billing companies may very well be located on United States soil.

There have been a number of cases in which law enforcement agents seized the billing records of these third-party billing companies. These databases contain information such as full customer lists with name, address, phone, e-mail, credit card numbers, name of Web site subscription purchased, etc. that was required by the billing site to verify the credit card purchase. Once seized, this information is distributed to local law enforcement and then to various jurisdictions for further investigation.

The use of such information gleaned from seized credit card verification databases was approved in *United States v. Gourde*.[19] Gourde had, for over two months, subscribed to an Internet Web site that contained images depicting minors engaged in sexually explicit conduct. The court held that those images were almost certainly retrievable from the defendant's computer if he had ever received or downloaded them, and that there was a fair probability that the defendant had received or downloaded images based on, among other things, the profile of collectors of such images.

Should a prosecutor get one of these cases, he or she should check on the background investigation by the billing agency before approving a search warrant. The agencies may have purchased a membership and downloaded content off of the suspect's purchased Web site. If so, the following questions should be asked:

1. Did the suspect, who subscribed to the site, know that it contained child pornography when he subscribed? Or does he have a reasonable argument that he might not have known?

2. Does it contain child pornography on the first ("splash") page? If so, clearly the suspect knowingly signed up for child pornography, which should provide probable cause for a warrant.

3. Does the text advertise child pornography in the contents? While the splash page may not contain actual illegal images, it might include text that promises illegal content once inside.

4. Has the suspect reported himself to be the victim of identity theft or credit card fraud? Much online child pornography financial transactions—indeed many online transactions in general—are completed using stolen credit cards. If such a theft was reported prior to the initial subscription, the prosecutor should proceed cautiously.

5. Does the information (e-mail address, home address, phone number, credit card number) match the suspect?

E. Referral by a Wife, Girlfriend, or Co-parent, Possibly During a Custody Dispute or With Some Other Reason for the Referrer to Be Disgruntled

Someone with a close personal relationship with the suspect may tip off law enforcement to child pornography possession. Sometimes this is a disgruntled ex-spouse or ex-girlfriend. Sometimes there is a child custody dispute between the suspect and his partner who "discovered" the pornography, or some other source of contention.

Prosecutors should proceed cautiously in such a case, while keeping in mind the possibility, however unlikely, that the disgruntled partner has deliberately put pornographic images on the suspect's computer in order to exact revenge, or obtain custody of a child. A proper forensic examination should rule this out as a possibility. Even if the disgruntled ex is being completely aboveboard and is only reporting what she has actually found, the defendant may exploit an ugly relationship to establish reasonable doubt.

1. Search issues

There is little expectation of privacy from other users in a shared home computer, such as a wife checking on her husband's late-night surfing habits. If so motivated, she may call law enforcement, show them questionable content if she has access (e.g., non-password protected material), and give them consent to search the computer. Since the defendant can withdraw consent at any time during the forensic exam, a search warrant for the computer should also be obtained to back up the consent.

2. Case law

a. *United States v. Brooks*[20]

The defendant claimed that officers exceeded the scope of consent when they searched his computer by means other then those explained to him in the course of obtaining consent, which were rejected. Officers told the defendant that they had ultimately used a specific software-driven search.

b. *United States v. Turner*[21]

A search of the defendant's computer files exceeded the scope of his consent to a search of his apartment in connection with an intruder's assault on a neighbor.

c. *United States v. Smith*[22]

The court addressed third-party consent to search a computer. In a very fact-specific holding, the court did not note any evidence that the defendant had password-protected the material seized from the computer.

d. ***Trulock v. Freeh***[23]

The court addressed third-party consent to search a computer where consent was given by another who had joint access to the computer but did not know the passwords, and therefore, did not have authority to grant access to the files.

e. ***United States v. Lemmons***[24]

An initial consensual search by police for a camera and recordings was subsequently expanded to the defendant's computer because the defendant voluntarily showcased pornographic Polaroids and turned on his computer for the officers.[25] The initial consent search of the defendant's apartment expanded to include his computer when an officer sat down at the computer and the defendant opened files for him and agreed to let the officer open the files himself.

f. ***United States v. Aaron***[26]

Police obtained consent from the defendant's live-in girlfriend to search the defendant's computer. Although the girlfriend had never used the computer, the court upheld the search finding that the defendant's failure to use passwords or actually prohibit his girlfriend from using the computer indicated her authority to consent.

g. ***United States v. Mannion***[27]

The defendant's wife's consent to search and seize a computer disk was valid where there was no evidence that the wife did not have complete access to those items.

h. ***United States v. Laine***[28]

The defendant's consent to a customs agent's and a uniformed police officer's entry into his home, where they subsequently obtained the defendant's written consent to a forensic examination of his computer and associated diskettes on which images of child pornography were found, was free and not coerced. In the early evening, they knocked on the door of the defendant's home, identified themselves to the defendant, and told him they wanted to discuss something that he probably would not want to talk about in public, brandished no weapons, uttered no threats, and resorted to no trickery to gain admittance.

i. ***United States v. Buckner***[29]

Courts have been leaning towards extending more protection to material on computers where an individual has taken the extra effort to protect it with a password. In *United States v. Buckner*, citing *Trulock* (see section "d" above), the court held that the defendant had a reasonable expectation of privacy in password-protected files contained on the computer he shared with his wife (who did not have access to the password-protected files, per the defendant). The court, however, upheld the search, stating that the

defendant's wife had apparent authority to authorize the search of the computer and did not have knowledge that any data contained therein was protected.

F. Pornography Inadvertently Discovered During an Unrelated Investigation (Fraud, Identity Theft, Etc.)

1. During an investigation of a child molestation case

There is a close and logical connection between the crimes of child molestation and child pornography. In the course of prosecuting a molestation case, evidence of child pornography will often be found on the suspect's computer. This pornography can then be used as the basis for additional charges, as well as serve as proof of intent in the molestation crime.

2. During an investigation of a non-sex offense

As in any case, child pornography may be discovered in the course of an investigation for a completely unrelated crime. The nature of computer use is such that it is perhaps more likely than ever that a fraud case will produce evidence of some completely unrelated crime, such as child pornography. This is because a computer will very typically hold material pertaining to every aspect of its user's life, as well as the lives of the user's friends and family.

If evidence of child pornography is uncovered during the investigation of an unrelated crime, it is **vital** to obtain the proper search warrants before continuing to conduct searches for additional child pornography. To fail to do so is to risk having crucial evidence of the sexual offense made inadmissible.

In *United States v. Carey*,[30] computers were searched pursuant to a warrant in a drug-crime investigation. The warrant authorized the search for evidence pertaining to the sale and distribution of drugs. The detective performing the search opened a JPG (image) file, and discovered that it appeared to contain child pornography. He then continued searching the computer, looking for further child pornography evidence. He did not first obtain a supplemental warrant. The defense brought a motion to suppress, which was denied by the district court, but reversed on appeal. The court of appeals held that the search for child pornography exceeded the scope of the warrant.

The detective's misstep came not from looking at image files. Image files may contain evidence of drug crimes, just as they may contain evidence of any crime. It was his admission that he changed the object of his search to a search for child pornography, without first obtaining a warrant that made his search excessive in the eyes of the reviewing court. Compare *Carey* with *United States v. Gray*[31] where the court held that viewing the contents of subdirectories containing child pornography, which then provided probable cause to obtain a second search warrant for child pornography, was within the scope of the original warrant concerning a hacker investigation. The key to the ruling was that the searching agent never abandoned his original search and knew of instances where files were intentionally mislabeled (e.g., text files in files with JPG extensions).

3. Case law

a. *United States v. Carey*[32]

The defendant was arrested on drug charges. The police obtained consent to search the defendant's apartment and seize two computers. A warrant was obtained to search the computers for evidence pertaining to the sale and distribution of drugs. A detective found JPG files, opened one, and saw child pornography. He then downloaded approximately 244 JPG or image files to disks. The motion to suppress was denied by the district court, but reversed by the Tenth Circuit: the search exceeded the scope of the warrant, but the court noted that the holding was very fact specific.

b. *United States v. Gray*[33]

Viewing contents of subdirectories that contained child pornography provided probable cause to obtain a second search warrant for child pornography, which was within the scope of the original warrant concerning a hacker investigation. The key to the ruling was that the searching agent never abandoned his original search and knew of instances where files were intentionally mislabeled (e.g., text files in files with JPG extensions).

VII. Varieties of Child Exploitation and Applicable California Charging Statutes

California statutes that prohibit child pornography have developed piecemeal over a number of years. As a result, the California statutes under which Child Pornography and Exploitation laws are charged lack consistency.

The applicable Penal Code sections contain duplicative language, are pled in the conjunctive, and allow the prosecutor wide discretion to charge appropriately based upon the facts. The most commonly charged (and easily understood) sections are set forth below:

Note: For a full breakdown of all child pornography laws and enhancements for certain crimes, please see the child pornography matrix by San Diego County Deputy District Attorney Jeffrey Dort and Deputy Attorney General Robert Morgester located at Appendix A.

A. Offense: Digital Images and Video Stored on Computers, Sometimes on Non-digital Media

Simple possession, Penal Code section 311.11(a), wobbler—misdemeanor or 16-two-three felony:

> Every person who knowingly possesses or controls any matter, representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, the production of which involves the use of a person under the age of 18 years, knowing that the matter depicts a person under the age of 18 years personally engaging in or simulating sexual conduct,

as defined in subdivision (d) of Section 311.4, is guilty of a public offense and shall be punished by imprisonment in the state prison, or by imprisonment in the county jail for up to one year, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by both the fine and imprisonment.

Simple possession with a qualifying prior, Penal Code section 311.11(b), two-four-six felony:

> If a person has been previously convicted of a violation of this section, or of a violation of subdivision (b) of Section 311.2, or subdivision (b) of Section 311.4, he or she is guilty of a felony and shall be punished by imprisonment for two, four, or six years.

Note: Only prior possession or manufacturing qualify as elevating priors.

B. Offense: Distribution of Child Pornography Via P2P (Peer-to-Peer File Transfer), E-mail, or Direct File Transfer

Penal Code section 311.1(a), 16-two-three felony:

> Every person who knowingly sends or causes to be sent, or brings or causes to be brought, into this state for sale or distribution, or in this state possesses, prepares, publishes, produces, develops, duplicates, or prints any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, with intent to distribute or to exhibit to, or to exchange with, others, or who offers to distribute, distributes, or exhibits to, or exchanges with, others, any obscene matter, knowing that the matter depicts a person under the age of 18 years personally engaging in or personally simulating sexual conduct, as defined in Section 311.4, shall be punished either by imprisonment in the county jail for up to one year, by a fine not to exceed one thousand dollars ($1,000), or by both the fine and imprisonment, or by imprisonment in the state prison, by a fine not to exceed ten thousand dollars ($10,000), or by the fine and imprisonment.

C. Offense: Possession with Intent to Distribute Via P2P, E-mail, Etc.

Penal Code section 311.2(b), two-three-six felony:

> Every person who knowingly sends or causes to be sent, or brings or causes to be brought, into this state for sale or distribution, or in this state possesses, prepares, publishes, produces, develops, duplicates, or prints any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, with intent to distribute or to exhibit to, or to exchange with, others for commercial consideration, or who offers to distribute,

distributes, or exhibits to, or exchanges with, others for commercial consideration, any obscene matter, knowing that the matter depicts a person under the age of 18 years personally engaging in or personally simulating sexual conduct, as defined in Section 311.4, is guilty of a felony and shall be punished by imprisonment in the state prison for two, three, or six years, or by a fine not exceeding one hundred thousand dollars ($100,000), in the absence of a finding that the defendant would be incapable of paying that fine, or by both that fine and imprisonment.

Under *People v. Cochran*,[34] a commercial purpose does not require that the defendant's trading of pornography be for making money. So, if the defendant is amassing his collection for trading it with others so that he can enlarge his own collection, this too qualifies as a commercial purpose.

D. Offense: Manufacturing (Using a Live "Model" in the Production of Child Pornography)

Penal Code section 311.4:

(a) Every person who, with knowledge that a person is a minor, or who, while in possession of any facts on the basis of which he or she should reasonably know that the person is a minor, hires, employs, or uses the minor to do or assist in doing any of the acts described in Section 311.2, shall be punished by imprisonment in the county jail for up to one year, or by a fine not exceeding two thousand dollars ($2,000), or by both that fine and imprisonment, or by imprisonment in the state prison. If the person has previously been convicted of any violation of this section, the court may, in addition to the punishment authorized in Section 311.9, impose a fine not exceeding fifty thousand dollars ($50,000).

[For commercial purposes, Penal Code section 311.4(b), three-six-eight felony (presumptive prison):]

(b) Every person who, with knowledge that a person is a minor under the age of 18 years, or who, while in possession of any facts on the basis of which he or she should reasonably know that the person is a minor under the age of 18 years, knowingly promotes, employs, uses, persuades, induces, or coerces a minor under the age of 18 years, or any parent or guardian of a minor under the age of 18 years under his or her control who knowingly permits the minor, to engage in or assist others to engage in either posing or modeling alone or with others for purposes of preparing any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film, filmstrip, or a live performance involving, sexual conduct by a minor under the age of 18 years alone or with other persons or animals, for commercial purposes, is guilty of a felony and shall be punished by imprisonment in the state prison for three, six, or eight years.

[For non-commercial purposes, Penal Code section 311.4(c), 16-two-three felony (presumptive prison):]

(c) Every person who, with knowledge that a person is a minor under the age of 18 years, or who, while in possession of any facts on the basis of which he or she should reasonably know that the person is a minor under the age of 18 years, knowingly promotes, employs, uses, persuades, induces, or coerces a minor under the age of 18 years, or any parent or guardian of a minor under the age of 18 years under his or her control who knowingly permits the minor, to engage in or assist others to engage in either posing or modeling alone or with others for purposes of preparing any representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film, filmstrip, or a live performance involving, sexual conduct by a minor under the age of 18 years alone or with other persons or animals, is guilty of a felony. It is not necessary to prove commercial purposes in order to establish a violation of this subdivision.

(d)(1) As used in subdivisions (b) and (c), "sexual conduct" means any of the following, whether actual or simulated: sexual intercourse, oral copulation, anal intercourse, anal oral copulation, masturbation, bestiality, sexual sadism, sexual masochism, penetration of the vagina or rectum by any object in a lewd or lascivious manner, exhibition of the genitals or pubic or rectal area for the purpose of sexual stimulation of the viewer, any lewd or lascivious sexual act as defined in Section 288, or excretory functions performed in a lewd or lascivious manner, whether or not any of the above conduct is performed alone or between members of the same or opposite sex or between humans and animals. An act is simulated when it gives the appearance of being sexual conduct.

(2) As used in subdivisions (b) and (c), "matter" means any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, or any other computer-related equipment or computer-generated image that contains or incorporates in any manner, any film, filmstrip, photograph, negative, slide, photocopy, videotape, or video laser disc.

(e) This section does not apply to a legally emancipated minor or to lawful conduct between spouses if one or both are under the age of 18.

(f) In every prosecution under this section involving a minor under the age of 14 years at the time of the offense, the age of the victim shall be pled and proven for the purpose of the enhanced penalty provided in Section 647.6. Failure to plead and prove that the victim was under the age of 14 years at the time of the offense is not a bar to prosecution under this section if it is proven that the victim was under the age of 18 years at the time of the offense.

VIII. State's Burden of Proof

A. Proving Material Depicts a Real Child

Since images of child sexual abuse are not illegal pornography unless they are photographic or video depictions of an actual child, anticipate the defense argument that the images are not "real"—that instead they are "morphed" or fabricated, completely computer-generated without involving the use of an actual child.

Digital animators and artists know that this argument is absurd on its face. The state of computer-animation technology as it exists today simply is not sufficiently advanced to allow the creation of computer images that are indistinguishable from photos of actual persons, much less movies or videos of persons.

Final Fantasy: The Spirits Within (H. Sakaguchi and M. Sakakibara directors, 2001) is often given as an example of the most advanced instance of completely computer-generated animated human characters to date. Yet even with the fact that the creation of *Final Fantasy* involved a multi-million dollar budget, thousands of man-hours by the most skillful computer animators around, and the images consisted entirely of clothed individuals, the resulting animated characters—while impressive—are still obviously computer animations.

1. Strategy tip: mix known images with images of unidentified victims

If there is any chance that the defense will attempt to argue that certain images are "virtual," one tactic is to include "known" images of child pornography (identified victims) in charging.

There are thousands of images of child pornography still in circulation that were manufactured several decades ago—well before digital-animation technology and personal computers. These images were manufactured and first traded when child pornography was distributed entirely in printed form, often originating in Scandinavian countries. These series often are identified by children's names, such as the "Jennifer Series."

Organizations like the National Center for Missing and Exploited Children as well as the United States Post Office, Customs Service, maintain collections of these images for law enforcement purposes. If a prosecutor believes the case involves an image that might be from one of these series, he or she should contact one of these agencies. If need be, they might be able to supply a witness who can attest to the fact that the images portray actual, identified victims who were minors when the images were first made. These images will be introduced at trial under the business records exception to hearsay.

2. Strategy tip: charge videos

Additionally, if a prosecutor is in possession of seized pornographic videos, it might be tactically wise to charge those as well, if doing so is practical. As noted above, the creation of a color, moving image of a child is even more technically improbable than the computer creation of a simple photograph.

If the case is in a jurisdiction where there is a high tech business presence, the prosecutor should attempt to find an individual with CGI (computer generated imagery) experience who could testify to the incredible complexity involved in the creation of a wholly digital image, much less a moving video.

B. Proving the Depicted Child Is Under 18

1. Difficulty of charging borderline cases

Unfortunately, many images depicting victims ages 13 to 18 cannot be charged. The reason for this is the difficulty in proving that the minor depicted is in fact a minor, if the individual is not identified.

All individuals vary in the rate at which they sexually mature. Because of family genetics, or certain racial characteristics, even adult women can sometimes look like young teenagers, and young girls can plausibly appear to be 18 or more years old.

In past prosecutions, a pediatric tool known as the "Tanner Scale" was sometimes used in trials for child pornography to establish the age of the portrayed victim. The Tanner Scale characterized typical stages of sexual development in persons of both sexes, based on pubic hair growth and breast size in girls, and genital size in boys. But the creator of the Tanner Scale has since repudiated its use for establishing an individual's age. As a result, it should no longer be used for this purpose.

Keep in mind the prosecutor's burden of proof regarding the victim's age when charging images. It benefits the prosecution that most child pornography collections are large. It should generally be easy to find representative images that a juror can easily determine as being a child less than 18 years of age.

2. No expert opinion required to prove victim's age

Based simply on their common sense and experiences with children, jurors are entitled to determine on their own whether a pictured victim is less than 18 years old. Proving that a child is a minor does not require expert testimony.[35] While a prosecutor might think it advantageous in some cases to enlist a pediatrician to testify as to the age of a depicted victim, there is also the danger that the pediatrician will waffle when faced with a picture of an individual who is obviously a child. The problem is this, a pediatrician is a doctor, and hence, a scientist. Scientists should be skeptical. If the prosecutor possesses a picture of a victim who is clearly a child, his or her case may be damaged if the prosecutor's pediatrician expert testifies only that the image is "consistent with the appearance of a child."

The bottom line is that the decision as to whether an image depicts a minor is based on the jurors' common sense and practical experience. Tragically, many images will be of tiny children—including toddlers and infants. A jury, especially one composed of parents and grandparents, will not question the age of the victims where this is the case.

C. Proving the Elements of Possession

In order to prove the state's case, the prosecution must establish that the defendant was in legal possession of the contraband material. Another way of putting it is that the defendant must be placed "at the keyboard" of the computer where the pornography was found—and that the defendant controlled or had the right to control material.

1. Definition of possession

The basic concept of possession is set forth in various CALCRIM instructions regarding the possession of firearms, controlled substances, stolen property, etc., but no specific instruction exists for the possession of child pornography. A special instruction tailored using the basic elements of possession and the elements of child pornography must be crafted for your jury. (A sample jury instruction is included at Appendix B.) If the material depicted does not show sexual conduct per se, but rather a "lewd and lascivious exhibition of the genitals" one should consider giving a further instruction on the *Kongs* factors, discussed previously, to assist the jury in their determination of whether the material was possessed for the sexual gratification of the viewer.

2. Proving possession

Any difficulties a prosecutor may face in trying to place the suspect at the keyboard will depend on a number of facts.

a. Number of persons with access to the computer and its pornography

i. Single suspect with family

A single suspect living with his wife and small children will often admit to the crime. But where he blames it on another member of this family, forensic and other evidence should be sufficient to rebut this defense.

The forensic data will reveal "metadata," data that is distinct from the actual content of the file. Put simply, metadata is "data about data." The metadata will indicate when files were downloaded or last accessed. This information can be used in conjunction with other forensic evidence to establish that the suspect did indeed control the files in question.

For example, if the files were downloaded (which is shown by the "created date" in Windows) at a certain time and date, other computer logs may show that the file was downloaded in close temporal proximity with other computer activities that are obviously attributable to the suspect. The computer may have e-mail records that show that an e-mail was sent at or about the same time as the file creation date, and that the suspect's e-mail account was the one being used. Or, forensic evidence of the Internet browsing history might show that certain Web sites were being accessed at the same time as the file creation date, and these Web sites contained material of known interest to the suspect—NASCAR, etc. The forensic evidence might also show that

the creation date matches a time when the suspect was logged in on the computer under his own account, possibly even a password-protected account.

ii. Single suspect living alone

Where the suspect lives alone, he might try to attribute the presence of pornography to viruses, Trojans, pop-ups, or other malware. The prosecutor will need a forensic expert to testify to the fact that no such malware was found on the searched computer. Furthermore, there is no evidence that any virus attack on a computer was ever responsible for placing child pornography on an innocent party's computer. To the extent that viruses and other malware alter a hard drive's file content, they will do so in predictable ways. They will **not**, for example, create complex directory structures on the hard drive, and organize files within those directories according to the "body type" of a child.

iii. House with many occupants or transitory occupants

Like other possession cases, establishing ownership may be difficult when dealing with a household with multiple transitory residents or users of a computer. In such cases, prosecutors will have to go beyond the circumstantial evidence resident on the computer. If there is a young boy in the household who also had access to the contraband-containing computer, showing that he did not download the images in question may require establishing, based on metadata, the time and date when the image was downloaded, and then using school records to show that the boy was in fact in school at the pertinent time. Similarly, employer's work records might be able to establish that other household residents were away from the computer when the contraband was downloaded or accessed.

Forensic examination is powerful yet still circumstantial evidence. In all cases, prosecutors will need to thoroughly prepare the case well before trial by conferring with a computer-forensics expert, and finding out exactly what he can testify to with respect to the evidence which was located on the computer—as well as (possible) conclusions that can be drawn from that evidence.

b. State of the files—deleted, not deleted, in unusual directories, with nonstandard file names

i. Deleted files

Are the owner and user of a computer in possession of pornographic images when those images have been deleted? Federal case law is split and California lacks authority on this subject.

Note: **Deleted files are not gone**. When a file is deleted from an operating system, it is not necessarily eliminated from the computer. If, in a typical Windows system, the contraband file is simply moved to the "recycle bin," the defendant is unquestionably still in possession of that file. The Windows recycle bin is simply another operating system directory with special characteristics.

Additionally, if the file is moved to the recycle bin, and the recycle bin is then emptied, the content of the file is still resident on the hard drive. The only change that is made with the emptying of the recycle bin—and the "deletion" of the file—is that the file information that allows the user to readily retrieve the file is removed or changed. The content of the file remains on the hard drive until it is eventually overwritten by other files that the user is actively manipulating, or by other disk-writing activities of the operating system.

In explaining this fact to the jury, a prosecutor should have the expert use an analogy, e.g., likening the computer to a (very) thick binder full of papers. The operating system uses those papers in the front and "tabs" them so they can be located quickly and easily. The "deleted" pages go in the back of the binder, and the tabs are removed. They may be disorganized and take more effort to locate, but they are still present in the "binder."

There are various places in the logical structure of the hard drive where deleted files may reside. Apart from the recycle bin, images may remain in the cache of Web pages used by Internet Explorer and other browsers to permit quick loading of Web pages that have been previously viewed. Additionally, the images may remain in the unused or "unallocated" space of the computer's hard drive.

In other instances, the files are not immediately accessible. When the recycle bin is emptied, retrieving the files is a somewhat specialized task—but it is still relatively trivial. There exists a number of commercially available and freeware programs, all available for download on the Internet, that allow the user to easily recover material from unallocated hard drive space. Using these programs, recovering deleted files can be done with a few clicks in a matter of minutes.

Explain to the jury why these "erased" files are still within the control of the computer user by using further analogies. Use analogies involving simpler, more familiar crimes, such as narcotics or possession of stolen property. Throwing a baggie of methamphetamine on top of a tall cupboard, or putting a cache of stolen power tools in a box under a house does not mean that owner is not in control of those items or that he lacks the right to control that property.

As noted throughout this chapter, the use of analogies is a powerful way of explaining complex computer processes in a way that the typical juror can understand.

Note: **Deleting files may cause loss of metadata.** Deleting files can sometimes cause the loss of the metadata that establishes when they were downloaded or last accessed. This can be problematic if the state's case relies on metadata to establish some element, such as the identity of the individual at the keyboard when the image was downloaded or accessed. But if the prosecutor elects not to charge the files that were deleted by the user, they can still constitute powerful evidence of intent, common plan or scheme, or most importantly in a child molestation case, evidence of the defendant's sexual attraction towards children. The date upon which files were deleted can also provide strong evidence showing consciousness of guilt. Often,

forensic analysis can provide the date upon which a file was deleted that could then be correlated to significant dates during the course of the investigation, such as the date the material was first discovered (e.g., by a spouse) or the date upon which the defendant was first contacted by law enforcement. An en masse deletion of child pornography or child erotica files closely following such a significant date is highly probative to show that he knew what he had was illegal and that he was attempting to hide it.

ii. Possession of deleted files: case law

Federal case law suggests two theories. First, having deleted child pornography files constitutes possession. Second, deleted files at least constitute evidence that the computer user possessed child pornography before the files were deleted.

The federal opinion in *United States v. Upham*[36] stated that a search warrant was not overbroad by allowing seizure of "any and all computer software and hardware … computer disks, disk drives." The original search warrant authorized recovery of previously deleted material; recovery of files attempted to be destroyed (deleted) is the same as decoding a lawfully seized coded message or reconstructing scraps of a torn ransom note.

The court in *United States v. Tucker*[37] held that the defendant knowingly possessed deleted cache files because he demonstrated ultimate dominion and control over the images.

United States v. Simpson[38] stated that the fact that a defendant deletes or destroys evidence does not eliminate his culpability for engaging in the conduct related to that evidence. In *Simpson*, the court held that there was substantial evidence that the defendant's computer contained two child pornography files, the names of which were substantially similar to the names of files downloaded by the defendant over the Internet, although the specific files listed in the indictment had apparently been deleted. The fact that the defendant deletes or destroys evidence does not eliminate his culpability for engaging in the conduct related to that evidence.

IX. Predators and Travelers

All child pornography users are predators in that their "hobby" is what permits the worldwide child pornography trade to continue to thrive. But offenders who also actively seek out meetings with children via the Internet are common. Too often, their aim is to meet and sexually victimize these children. The common term for these types of offenders is "travelers." Traveler cases usually do not result from parent referrals, but are normally the outcome of undercover stings.

These predators are generally extremely cunning and use any number of ploys to lure their victims into a meeting. Often the predators are well-versed in youth culture. In chat rooms they may use the abbreviations common in online chat and instant messaging. Most people who have used chat rooms on more than a few occasions are familiar with a handful of these abbreviations. In fact, hundreds of these abbreviations exist, and by using them, predators may make it appear that they are younger than they really are.

Sometimes these predators make no bones about the fact that they are adults, although they might exaggerate their ages downward on the theory that a 14-year old is more likely to chat with a 35-year-old than with a 55-year-old.

Predators who actively attempt to arrange meetings with their young chat partners will often travel great distances, even hundreds of miles or more. Their intention, of course, is usually to sexually abuse these children. Fortunately, many of the "children" these predators end up meeting are undercover officers instead.

A. Charging Statutes

Prior to 2006, there was no California "traveler statute." Travelers were commonly charged under Penal Code sections 664 and 288, under the authority of *People v. Reed*[89] and other "charm school" cases, in which the defendant travels to a certain location with the expectation of having sex with a minor child. Since the minor does not actually exist in undercover-officer cases, the cases were always charged as an attempt (where impossibility is not a defense). Since the inception of Penal Code section 288.3, commonly referred to now as "luring," the law has changed, but the practical issues regarding traveler cases remain. The prosecutor can always use Penal Code section 288.3 when the suspect has not actually engaged in any active "overt act" in furtherance of having sex with the target such as driving to a meet location, making hotel reservations, etc.

B. Questions to Evaluate the Strength of a Traveler Case

1. How far did the traveler in fact travel in order to meet the victim?

Clearly, the offender who expresses an interest to have sexual contact with a child and then drives 400 miles to meet him is likely to be serious about carrying out his intent—just as the car buyer who drives 75 miles will more likely be a serious shopper than the buyer who walks across the street to view the same vehicle.

2. Did the traveler do something beyond "mere solicitation?"

The traveler suspect must commit an act beyond mere solicitation. But when the specific intent of the suspect is clear, only slight acts are necessary.

3. What did the traveler bring to meet with the child?

When the traveler arrives at the meeting place, often the suspect will come weighted down with material evidence of his sexual intent in meeting the child. Did the suspect come "prepared" (lube oil, condoms, toys, etc.)? Clearly, a traveler who claims that he did not intend to have sexual contact with a child will be hard pressed to explain the presence of sexual aids in his possession at the time of the meeting. Also, a traveler who claims he was living out a fantasy, and actually believed his victim was an adult may find it harder to explain having toys and candy.

4. **Did the suspect send pornography to an undercover officer or child?**

   If so, regardless of the traveler's intent, the suspect has violated Penal Code section 311.1 if the material transferred is child pornography. If the traveler's intent was to seduce, the suspect has violated Penal Code section 288.2 (or attempt section 288.2 if an undercover officer was involved).

   Note that under Penal Code section 288.2, the "harmful matter" need not be child pornography. Furthermore, the definition of "harmful matter" is target-specific, i.e., what is harmful for minors. Thus, it is a crime to send adult pornography to a child, but **only** if it is done with the intent to seduce.

   The intent to seduce may include intent to induce a child to sexually stimulate himself alone. An alternative charge, Penal Code sections 664 and 288, attempting to get a child to touch himself/herself over a phone line can constitute attempted child molestation,[40] but this was apparently not charged in *People v. Jensen*.[41] The court in *Jensen* found that while the material sent to the minor was indeed harmful, the acts themselves never amounted to anything resembling an "attempt" to meet and have sex with the child.

5. **Is there any chance a jury could believe the predator's defense that "it was all just a fantasy?"**

   A good rule of thumb is if it seemed too easy then it probably was. Beware the "45-minute traveler." "Real children" need more than 30 minutes of cajoling before agreeing to meet a stranger. Some individuals may truly believe they are role-playing.

6. **Was there adult pornography recovered that suggests fantasy? Was there child pornography recovered on the suspect's computer?**

   There is much "mainstream" pornography available online that features adult women dressed like the stereotypical schoolgirl with plaid skirts, knee socks, pigtails, and so on. Finding such material on the suspect's computer could indicate any of a number of things. It could, for example, indicate that the suspect actually does engage in role-playing/fantasy types of behavior, in which he fantasizes that his sexual partner is a naive schoolgirl. At the same time, it could indicate he has a sexual attraction toward preteen girls. In any case, if this type of material is found on the computer—but no actual child pornography is found—a defense attorney could plausibly make that argument.

   Of course, it could also indicate that the suspect is a potential predator, and that he has been cautious enough to either refrain from downloading child pornography, or shrewd enough to not to be caught with any. In any case, prosecutors should remain aware that the fantasy defense could be raised here. Did the suspect engage in role-playing as evidenced by other chats recovered from computer? If other chats were logged and stored on the suspect's computer, their content may provide evidence that the suspect did have a habit of engaging in online "role-playing." In some instances, the defendant's penchant for role-playing will be obvious—for example, where he pretends to be a vampire or a rock star talking to a groupie.

7. **Did the suspect ask the undercover officer if he or she was law enforcement? How often?**

   The fantasy defense is less tenable if, during the course of the chat, the suspect asks whether the "child" with whom he is chatting is law enforcement. A surprisingly large number of suspects will ask this question, believing that law enforcement are obligated to answer truthfully.

   When the "are you sure you're not a cop?" question is asked, it is powerful evidence that the suspect did not believe he was harmlessly engaging in a depraved fantasy with another adult. It shows that he was aware that what he was doing was illegal by the very fact that he was concerned that law enforcement might be on the other end of the line.

8. **Did the telephone conversation made during the sting plausibly involve a minor?**

   In some undercover operations, the operation will involve going beyond a mere text-based chat, and the suspect will ask to speak to the child to reassure himself that he is in fact speaking with a child, and not a cop.

   In instances such as those, the undercover decoy who plays the role of the child might be a female officer whose voice can easily be taken as that of a boy or a younger girl. Devices are also available that alter the pitch of a speaker's voice so that an investigator with a lower voice of an adult can pass himself off as a minor while on the phone.

9. **What does the sting telephone call sound like?**

   When an undercover decoy is used to make a "sting" telephone call, a prosecutor must objectively review the recorded telephone call, and ask the following questions: What would a jury think? Did the undercover officer convincingly sound like a child? Was the level of the "child's" language consistent with her purported age? Or did she sound sophisticated and experienced?

   If there is reasonable doubt that the suspect believed he was going to meet a real child, do not charge the suspect.

10. **Did the predator actually meet his victim? Did he send "harmful matter" with the intent to seduce (*no intent to seduce; no crime*)?**

    Even if there is no meeting between the online predator and the victim, it may be that a crime has been committed in the course of the online chat. For one, if the content of the chat is sexual and if the predator has sent "harmful matter" to the victim with the intent to seduce the victim, then he has completed a crime. Additionally, under Penal Code section 288.3, the mere act of setting up a meeting with a child or a person the predator assumes to be a child is a crime. There is no requirement that the predator actually meets the child or the person the predator assumed to be a child.

11. Is the evidence strong?

In the under-prosecuted world of child pornography and travelers, dedicate prosecutorial resources wisely. Expend valuable time and effort on obviously dangerous individuals, against whom the evidence is strong. Their dirty world is teeming with their kind; throw the lightweights back into the water and fish out someone truly predatory.

Look for alternatives for transmitted content[42] where age is irrelevant. If no attempt was made, consider a Penal Code section 647.6 misdemeanor for his efforts.

X. Solicitation and Attempt

Penal Code section 653f, governing solicitation, does not apply where the defendant directly solicited the minor to "commit" the offense of lewd or lascivious acts. Since the minor would not have committed the offense of lewd or lascivious acts by doing what the defendant asked and the acts were not crimes to the minors.[43]

Note: Recently prosecutors have run into problems using the attempt statute to prosecute traveler cases (charging Penal Code sections 664 and 288.3), a problem obviated by the enactment of Penal Code section 288.

Judges have ruled that the suspect's conduct constitutes solicitation but does not rise to the level of attempt. In summary, solicitation is an offer or invitation to another to commit a crime.[44] It does not, by itself, constitute an attempt, but may escalate into an attempt to commit a crime after the officer commits "a direct, unequivocal act towards committing the crime [.]"[45]

It can be extremely difficult to show the necessary act for a violation of any attempt statute in traveler cases.[46]

Since there is no solicitation offense available to charge, prosecutors are urged to consider filing additional alternative charging theories such as Penal Code section 288.2 [sending defined harmful matter to the child for the purpose of seducing the minor] or Penal Code section 207 [enticing or persuading a child to move within the county for purposes of committing an act as defined by section 288].

XI. Child Molestation Cases

Remember that the ultimate goal of a child pornography case is not to control the thoughts or predilections of the offender. The ultimate goal of any child exploitation case is to protect children, wherever they may be—those previously victimized, as well as those at risk of becoming victims.

Check carefully for any indication that the target produced the material locally. Check the images for recognizable local landmarks or topography. Check to see if the images show areas of the defendant's residence, inside and outside, and surrounding areas.

Also, check to see if the digital files themselves contain metadata that can identify the camera that made them. Digital camera files will often include information that include the make and model of

the camera, the serial number of the particular camera that was used in taking the pictures, the dates and times when the pictures were taken.

Anything found that suggests inappropriate behavior should lead to an immediate forensic interview of that child; the converse is true for any case involving sexual abuse of child.

If any witness (victim, wife, girlfriend, etc.) suggests defendant spent an inordinate amount of time on a computer, the case agent should be able to swear out a search warrant for the computer, based on his or her training and experience.

Child pornography is now commonplace among individuals who both molest children and own a personal computer. But if the suspect does not own a computer, does not use one frequently, or if a witness has never seen him use it, obtaining a warrant will be more difficult. In those instances, explore alternatives such as a consent search authorized by the defendant's spouse or cohabitant. Assuming the spouse or cohabitant is both cooperative and has unfettered access to shared computer, getting a valid search based on consent should not be problematic.

As always, undertake to obtain a consent search discreetly. If the suspect knows an investigation is going on, he may try to delete, erase, or wipe data. If this is not done correctly with effective software, evidence may still be recovered, as it is difficult to erase all traces of evidence of pictures, videos, Internet history, drop-down menus, auto-compete forms, etc. Additionally, deleted pictures in child abuse cases are perhaps more valuable than the non-deleted material, as the jury can see inside the defendant's sexual mindset and what is a serious indicator of consciousness of guilt. Traces of deleted file names that suggest child porn can also be recovered that are highly indicative of an illegal sexual intent (e.g. a video cache entitled "Dad Fucking His 10-Year-Old Daughter.)[47]

It is nearly impossible without the use of a good wiping program to clear out all traces of inappropriate activity on a computer. There are many ways a computer-forensics expert can trace the browsing and computer habits of a child molester or child pornographer: Internet history (Web site addresses, "cookies," data files, auto complete forms, cached file names, etc.). Even if the material is not visual in nature and cannot be charged, it may be admitted under Evidence Code section 1108 specifically to show the defendant's propensity for this type of activity, as section 311 charges and section 288 charges are specifically mentioned within the types of offenses covered by Evidence Code section 1108.

XII. Search Warrants and Staleness

Child pornography is unlike other forms of contraband, much of which is inherently transitory. Contraband, like drugs and stolen property, is always in flux—being sold or consumed. When a stolen car is sold, or drugs are consumed, they are gone. Child pornography, by its nature and the nature of its collectors, is different.

First, collectors treasure their collections and rarely completely discard any part of them. Even if the collector is interested in boys exclusively, he will still maintain vast quantities of images of underage girls indefinitely. These images have value to him in two ways: (1) he can use those images in trade for images more to his liking; (2) he can use those images to facilitate a molestation, to "prove" to his victim that sexual activity by minors is normal and acceptable, or to gain the friendship of his male victim.

Second, duplication of pornography is essentially cost-free, fast, and effortless. With the ever-decreasing cost of hard drive storage space, even hundreds of thousand of files can be kept on a single, inexpensive hard drive.

In short, there is no reason for a child pornography collector to destroy material, and so they rarely do. The child porn collector with a certain set of images on a given date, he will almost certainly still have those images, as well as many more, months and years later.

As a result, search warrants should always contain a "staleness" paragraph explaining why the affiant believes property is still there despite the passage of time. A standard boilerplate, however, will not be sufficient, particularly when 10 or more months have passed from the time when the suspect was known to be in possession of the pornography in question. The affiant must express his opinion, and the bases for that opinion, and if possible, cite particular examples of how the long property sought (child pornography) has been found at other offenders' homes before its discovery in a search. The longest period approved (10 months) in published case law is found in *United States v. Lacy*.[48]

XIII. Peer to Peer File Sharing

Peer to peer (P2P) networks first came to the public's attention during the controversy over the first large P2P file-sharing network, "Napster." Napster, which thrived in the late 1990s, was the means by which complete strangers swapped thousands of copyrighted songs online.

The principle behind P2P is that individual users may "share" files over a network created by specialized software. In a typical office network, the computers that comprise the network function as either clients or servers. To put it simply, servers are the main repositories of data that the company accesses and works on. The clients are the workstations that the employees use to access the server-based files. By contrast, in a P2P configuration, each computer is equally a client and a server.

In the earliest days of online child pornography, users of child pornography would often become members of a Bulletin Board Service (BBS). A bulletin board service would work as follows. The bulletin board operator would own one or more computers that stored pornography. The customer would download the pornography over a telephone line using a modem. In this case, the remote system operator's computer with the stored pornography was functioning as a server, while the customers' computers functioned as clients.

By contrast, in P2P networks, each individual's computer contains some of the child pornography (or adult pornography, pirated music, pirated movies, etc.). If user A wants a particular photograph and user B wants a different photograph, they likely will not end up downloading it from the same computer since the content is distributed over tens of thousands of computers.

Each user of a typical P2P network has the option of sharing content on his own computer, or "leeching"—seeking to download content from others, while providing no access to his own local files. So what incentive does any user have to share his files—especially if sharing them is illegal and puts him at risk of prosecution? There are at least two answers. First, those who allow uploading or sharing often gain special privileges within the network. For example, they get faster data-transfer rates, so that they can download large files in less time. Others seem to obtain some enjoyment by flouting the law. Another characteristic of P2P networks is that a user can upload a single file from

several different users who have local copies of an identical file. For example, if a user is downloading a movie on Napster, that user might be downloading it from a dozen or more people simultaneously, each user providing a fraction of the total data. This presents occasional evidentiary issues.

Hash Values

How is it possible that a software program can determine that a dozen people who are online with a certain photo to share, all in fact have the same photo—even if each of them has named it according to a different convention? This is because software identifies a file not on its name but rather on its "hash" value.

The hash value of a file is like a file's "digital fingerprint." If two files—say two photographic images—have the same hash value, then they are identical—the same dimensions, the same color content, the same subject. No two different computer files are comprised of the same coded series of numbers. As noted elsewhere, a computer file consists of a large number of zeroes and ones.

Law enforcement may have software that seeks out known child pornography images and videos, catalogued by hash value. The search function of the software can find known child pornography files (usually videos) by their hash value and categorize them geographically by using the IP address, also logged by the software. Once the IP address at which the file is being shared is established, the investigating officer can issue a search warrant or administrative subpoena to the ISP requesting the subscriber information of the individual who was assigned the IP address at the time it was displaying the known child pornography file(s). Once this information is obtained, additional background investigation can be completed and a search warrant obtained for the residence, computer, e-mail accounts, etc. Such operations have met with great success not only in California but in Wyoming and New Jersey as well, with child pornography being found in a very high percentage of the residences searched. As with all child pornography cases, however, the information takes time to develop and accordingly, so do the procedures necessary to investigate the case correctly and obtain a search warrant. Thus, the affiant in such a search warrant should devote at least a paragraph detailing why he or she believes, despite the passage of time, the property sought will still be at the location requested to be searched. Since the terms and methods used in a P2P search warrant may be complicated, have the affidavit reviewed by a colleague who is not particularly versed in computers or technology. See if they can understand the affidavit as written by the officer. If they have difficulty, return the affidavit to the officer for "dumbing down" or more politely put, "simplification" of the more "techy" terms and procedures described in the affidavit.

A. Peer to Peer Architectures[49]

Peer-to-peer file sharing is a decentralized file-sharing technology that enables Internet users to swap legal as well as illegal computer files. The term "decentralized" refers to the fact that there is no single "central" repository of files accessible to downloaders like there is, for example, on a Web site with links to downloadable MP3s or movies. In contrast to such client-server architecture, each user in a P2P network can function as both a client and a server, and each user's computer has equivalent capabilities and responsibilities within the network.

Currently popular P2P programs allow Internet users to trade not only MP3s but also any kind of computer file, and P2P has now become one of the primary means by which pedophiles share child pornography.

Additionally, the growth in the popularity of broadband access means that relatively large files, including copyrighted software applications and full-length movies, are now heavily traded.

Roughly categorized, there are three types of Internet P2P architectures:

1. **Centralized indexing systems**

   In its original form, Napster used this type of indexing system. In a centralized indexing system, one or more servers host compiled lists of the files that the individual users are sharing.

2. **Completely decentralized indexing systems**

   In this type of system, each user's computer indexes only the files on his or her computer.

3. **Supernode systems**

   In this system, a number of computers that are online at any given time are designated as indexing servers and will host the file indexes for all other users' computers. Whether or not any given computer is designated as a supernode will depend on that system's characteristics: processing power, connection speed, and so on. Any online user's computer may be functioning as a supernode—he or she will typically be unaware of this fact.

B. Peer to Peer Investigation Techniques

Searching for child pornography is straightforward. If the user transfers child pornography to law enforcement, officers have the ability to capture the IP address and, after obtaining the subscriber's records, hopefully obtain the user's location. Simple possession of child pornography is a now a felony "wobbler." If a user is sharing, however, he or she was arguably trading child pornography—a felony. But proving a violation requires proof of intent to distribute. Most P2P applications share downloaded files by default. Therefore, to establish intent to distribute, ideally the prosecutor would be able to present circumstantial evidence of such intent. Examples are e-mails or chat logs in which the user communicated with others about his or her collection.

1. **Going online**

   First, go online using a registered copy of the P2P application that has been selected for the investigation. Registration of P2P programs is generally free, although some P2P companies offer premium services that require payment. In any case, an investigator would not want to have to testify that he or she was using an illegitimately obtained or "cracked" version of the file-sharing program during the investigation.

2. **Searching**

   Once online, search for contraband files. Searching for these items is largely self-explanatory. Using, for example, "Photoshop" as a search term will return a list of users who are sharing

(or at least claiming to share) a version of the copyrighted graphics application Adobe Photoshop. Searching for contraband child pornography will require the searcher to use standard search terms such as "Lolita," "tinies," "young girls," etc.

Just because a file looks like child pornography does not mean it actually is. Examine each file in its entirety to make sure it is what it claims to be. Another issue concerns the technology used to conduct the initial search. The investigation must not invade the privacy of the P2P user under investigation. Therefore, consider whether the technology used in the investigation is available to a "normal user." If a normal user, not a hacker, has access to the same information as law enforcement, there should be no invasion-of-privacy concerns.

3. Identify the user

In order to identify the person offering the file, identify the IP address of the contributor. (Tiny personal firewalls will provide this data.) Further, he or she has no right to privacy in this information, so no legal process is required.

The file itself can come from multiple contributors. In order to speed downloading, P2P applications enable simultaneous downloading of different segments of the file from different users. If this is occurring, the application will make this apparent and will show the usernames of all individuals participating in the file transfer.

If a file is downloaded from multiple users at once, this will eventually create evidentiary issues with respect to testimony. At best, a prosecutor will be able to make the claim that any given file trader provided only a part of the contraband file. The prosecutor will need someone to explain (whether in a search warrant application or in courtroom testimony) how the P2P application works and that although the defendant only provided a segment of the file, he or she in fact must have possessed the entire file.

Next, perform a WHOIS query on the obtained IP address. (Try the Web site *www.samspade.org* for links to this and other services.) The IP address may resolve to some overseas country, very possibly one with which law enforcement cooperation is problematic. In any case, if it is determined that the computer hosting the files in question is overseas, it is likely that a prosecutor will have to make the decision to allocate his or her resources to investigating a more accessible target.

Note: Many law enforcement agencies have access to software that searches files hosted on a P2P network and narrows the user's location to a certain area by identifying a unique block of IP addresses that are used in that region. This reduces the scope of the investigation to a known population within a limited geographical area, such as the Sacramento Valley.

XIV. Discovery Issues and Presentation at Trial

A. Use a Protective Order

Prior to *Westerfield v. Superior Court*,[50] traditional discovery of child pornography images and video was not practiced, and typically, copies were **not** made available for the defense's

(somewhat) unfettered use. Rather, the defense would be required to conduct any necessary review of the contraband at a law enforcement facility only.

Since *Westerfield*, discovery is made under extremely limited circumstances and always pursuant to a protective order signed by the prosecutor, defense attorney, and judge. The protective order should always

- limit the defense attorney's uses of the material;
- require that any expert hired by both, sign and be bound by the same order; and
- require that all illegal materials turned over in discovery be returned within 10–30 days of a case's completion.

B. Presentation of Evidence at Trial

1. Decide between digital files and hard copies

Exhibits can be prepared for court and the jury in either printed or digital form. The approach the prosecutor chooses will be a function of what his or her budget permits, what is most convenient, and other practical considerations. For preliminary examination, PowerPoint slides or printed images may suffice. For presentation to juries, it is usually impractical to produce 13–15 copies of each image charged, so arranging for digital projection of the images is usually the better option.

2. Protect victim anonymity during trial

While the trial is, of course, a public hearing, argue to the court that the public has no right to view illegal material, and that in the interests of protecting the victims from further exploitation, all child pornography images that are presented to the jury should be presented in a way that does not make them viewable to courtroom observers.

To accomplish this, the prosecutor should request permission to cordon off half of the courtroom audience area. Position the projection screen so that images are visible to the court, counsel, and jury but not the audience. Attempt to arrange it so that the audience sits nearest to the screen, and to its side—at an angle that makes viewing the screen as difficult as possible. But the audience should still be able to see the witnesses as well as counsel.

Depending on the particular layout of the courtroom, it may not be possible to prevent the audience from seeing the images completely. But if the viewing angle is extreme, it will be difficult or impossible for audience members to make out identifying details of the victim's faces. If that is the case, at least the prosecutor has done everything possible to limit the victims' further exposure and humiliation.

3. Preserve PowerPoint presentations on CD-ROM (including all source files)

If a PowerPoint presentation is used in the course of the prosecution's trial presentation, the prosecutor should make sure that all "source files" are included on CD, as well as the PowerPoint presentation itself. The reason for this is that video files may not play on another

computer unless the source files are within the same directory, or at the very least, located on the same disk. Also, digital quality may suffer in presentation if details are important. Each slide in a PowerPoint presentation should contain both the specified file name as well as the count number to which it corresponds.

4. Seal exhibits

Finally, make a motion to seal all exhibits—the prosecutor may do this immediately after admission of the evidence, or at the trial's end.

The prosecutor's computer-forensics expert should provide a disk (DVD or CD) containing all "questionable" material, including where the material was found, how it was probably obtained, and whether or not any questionable material was "shared" via e-mail, direct file transfer, or one of the many "peer to peer" (P2P) file-sharing networks.

All information contained within a standard computer, if printed, would easily fill a room, so for obvious reasons, the computer-forensics expert is needed to cull the relevant material from the overwhelming amount of irrelevant data every computer contains.

5. Computer forensics expert's testimony and demeanor at trial

The computer-forensics expert should remain as neutral as possible and analyze data in a scientific, objective manner. Interpreting the results is best left to when the analysis is combined with the other evidence (suspect interviews, etc.).

The prosecutor should prepare with the computer-forensics expert to ensure that he or she will be able to explain complex concepts in a simple manner. Be wary of a computer-forensics expert who, naturally and unintentionally, wanders off into technical areas far beyond the grasp of not only the prosecutor, but also jurors. If the prosecutor allows this to happen, the audience, as well as the case, could be lost.

Watch jurors as the computer forensics expert testifies. If anyone looks bewildered, tell the expert to stop, back up, and translate his last bit of testimony into common English. Never be afraid of the DID (Dumb It Down) concept. (See sample computer-forensics-expert questions at Appendix C.)

C. Understanding Basic Computer Forensics

A qualified computer-forensics expert is necessary to explain computerized evidence to a jury. He or she must be experienced in using the forensic software that was employed in the investigation of the case.

A prosecutor must know something about computer forensics. The following is an overview of the issues that a prosecutor's computer-forensics expert should be able to address at trial, issues of which the prosecutor should also have a working technical grasp.

The computer-forensics expert should explain the following.

1. **He did not search or work on the suspect's computer directly**

   When a computer-forensics expert makes a forensic examination of a computer, he does not simply "boot" the computer up. The reason for this is that the evidence he examines **must** be unaltered from the state is was in when it was in the suspect's possession.

   When a sample of cocaine is introduced into evidence in a drug case and testimony is given that it is the very same substance that was found in the possession of the suspect that constitutes proof that the defendant was in possession of cocaine. Handling computer evidence, however, presents issues not found in a drug case. Every time a computer is started up thousands of files are altered in very small ways. For that reason, it is imperative that the computer forensics expert who examines the computer use a "write blocker"—a device, either software or hardware, which prevents changes from being made to the original computer's hard drive.

   Windows operating system files are vulnerable to unintentional change if accessed via the operating system. For example, each Windows file has associated metadata that indicates when that file was created, last modified, or last accessed.

   In a child pornography case, an important part of proving that the defendant was the individual who downloaded and viewed the pornography may rest on the prosecutor's ability to prove that a given file was last accessed on a certain date, when the suspect was know to be in control of the computer. If the prosecutor's computer forensics expert is forced to testify that the computer evidence was unintentionally altered, and does not mirror **exactly** the state of the hard drive at the time it was seized, then a claim that an access date proves something meaningful about a given file could be undermined. For example, the defendant may argue that he purchased the computer second-hand—and had no idea that it held 20,000 images of child sexual abuse.

   If the prosecutor's computer forensics expert can show that the files were created well after the date on which he claims he first came into possession of the computer, this would effectively refute the defendant's argument.

   Note that in Windows, a file that is downloaded has a file system creation date and time that corresponds with the date and time it was transferred from a remote hard drive to the user's hard drive. This is because the file itself literally is created at that time, insofar as the downloading computer is making a "new" digitally precise duplicate of the file on the remote computer. But other types of metadata can also be retrieved from recovered files. For example, most current digital cameras include with the digital-picture file metadata that contain a wealth of information: the make and model of the camera, the camera serial number, the date and time when the picture was originally taken, the camera settings.

2. **The network setup of the defendant's computer**

   Was the defendant's computer connected to a network? If so, what kind, and what was the nature of the connection?

Almost certainly, the computer had Internet access, which means simply that it was connected to the huge global network that is the Internet. But it is also important to know if it was connected to a smaller local network—for example a LAN in the workplace or home.

Furthermore, it is important to address whether the connection was wired, or wireless. Hard-wired and even wireless home networks are now common and cheap. If the defendant maintained a wireless home network, or had a wireless access point at his home or place of work, the defense could argue that an outside party, even someone located in a van parked outside the defendant's house, accessed the network through the wireless access point without permission, and placed files on the defendant's computer. For that reason, it is **vital** that the computer-forensics expert address what kind of security was in place on the network in question.

3. **Trojans, viruses, malware (what they do, and whether any were found on the defendant's computer)**

A prosecutor's computer-forensics expert should explain how Trojans, viruses, and other malware work, where they come from, and what they are. The defendant might claim that malware "planted" child pornography on his computer. The prosecutor's computer-forensics expert should be able to refute this defense, based on various factual findings resulting from the forensic examination.

Highly organized directory structures indicating that the computer user sorted and maintained his collection are not consistent with any known computer malware. Instead, they demonstrate that the computer user was actively maintaining his collection.

Additionally, changed file names can refute the defense argument that an outsider surreptitiously placed the images on the defendant's computer. A low-tech and unsophisticated method of concealing a file type is by changing or deleting its extension, so that an image or video file is not recognizable by the casual computer user. For example, a JPG file is a common type of image file, which ends with the extension "jpg." The pornography collector might change the extension to "MP3"—making the file **appear** to be an audio file. File renaming like this is not consistent with any known virus and is evidence of consciousness of guilt on the part of the computer user who made that change.

If the defendant claims that the child pornography on his computer is the result of a redirect or "pop-up," the fact that the image is located in a directory apart from the browser cache will rebut this claim. The prosecutor's computer-forensics expert should be able to explain the difference between a "URL" (Web site address) that has been deliberately accessed by the computer user through a browser, and a "redirect" (pop-up ad).

The forensics expert will likely use forensic software to perform searches for strings of text on the hard drive. Searching for "preteen" may locate not only pornographic images with matching filenames—but also possibly the text of e-mails created by the computer user that have been stored on the hard drive, either through deliberate user actions, or as a result of operating system processes outside of the control of the casual user. Clearly, evidence that the

defendant was using e-mail to boast of his collection of preteen hardcore pornography would rebut a claim that he had no idea that such material was on his computer.

Forensic software also has tools for parsing out and analyzing the computer user's Internet history and the existence of cookies and other data files that leave an evidentiary trail that helps to trace the user's Internet footsteps.

The following is a summary of the steps taken by the prosecutor's computer-forensics expert and what the expert will look for to refute the defense's arguments that another person is responsible or that the defendant did not have knowledge of the child pornography.

- Defendant's computer is "imaged" by the computer-forensics expert, making a bit-for-bit copy.
- The copy can then be analyzed without changing files.
- Many child pornography collectors maintain organized file "tree" structures.
- Many hide them in obscure files or deep within operating system files.
- A computer forensics expert can parse them out and explain how and where they were located.
- File locations may also defeat an "automatic" (and thus unknowing) download defense if raised.
- Forensic software does not use a computer's operating system. It finds material in unused space that may have been "deleted." (See sections "b" et seq., beginning on page VI-20, for an explanation of active and unused space and how it relates to the concept of possession.)

XV. Sentencing and Forfeiture

All felony child pornography and most misdemeanor exploitation charges are mandatory Penal Code section 290 offenses. Some are prison presumptive, others are mandatory prison, including the use of child pornography in a child molest. (See matrix at Appendix A.) Any computer equipment, including all peripherals used in a sex crime against a child is subject to forfeiture per Penal Code section 502.01. If the computer belongs to the defendant, have the defendant waive his statutory right to a forfeiture hearing before the sentencing judge under Penal Code section 502.01(c). This hearing is civil in nature, which means that first, the defendant is not entitled to a court appointed attorney, and second, he may be called as a witness. Since the burden of proof is a preponderance of the evidence and the conviction stands as proof beyond a reasonable doubt of the crime, almost all defendants and their attorneys waive their right to such a hearing and stipulate to forfeiture of the equipment. If the computer belonged to another, the equipment is subject to forfeiture only if the owner knew it was being used for specified illegal acts. This is a rare case, usually involving a complicit or protective spouse. These factors motivate almost all defendants to waive expensive, unnecessary, and humiliating forfeiture hearings, and stipulate to forfeiture of the computer equipment. Any plea to these offenses should involve such a waiver and stipulated forfeiture. (See sample forfeiture order at Appendix D.)

ENDNOTES

1. *New York v. Ferber* (1982)458 U.S. 747.
2. "[A] style of animation originating in Japan that is characterized by stark colorful graphics depicting vibrant characters in action-filled plots often with fantastic or futuristic themes. Merriam-Webster's Collegiate Dictionary (11th ed. 2005) p. 49, col. 2.
3. *People v. Kongs* (1994) 30 Cal.App.4th 1741.
4. *Id.* at 1755.
5. *United States v. Jacobsen* (1984) 466 U.S. 109.
6. *Id.* at 115. See also *United States v. Miller* (8th Cir. 1998) 152 F.3d 813, 815–816; *United States v. Donnes* (10th Cir. 1991) 947 F.2d 1430, 1434. But see *United States v. Allen* (6th Cir. 1997) 106 F.3d 695, 699 (dicta) [stating that *Jacobsen* does not permit law enforcement to reenact a private search of a private home or residence].
7. *United States v. Hall* (7th Cir. 1998) 142 F.3d 988.
8. *United States v. Barth* (W.D. Tex. 1998) 26 F.Supp. 2d 929.
9. *United States v. Grimes* (5th Cir. 2001) 244 F.3d 375.
10. *United States v. Simons* (E.D.Va. 1998) 29 F.Supp. 2d 324.
11. *Muick v. Glenayre Electronics* (7th Cir. 2001) 280 F.3d 741.
12. See also *United States v. Angevine* (10th Cir. 2002) 281 F.3d 1130.
13. See also *United States v. Reilly* (S.D.N.Y. 6/3/02) 2002 WL 1163572.
14. *United States v. Slanina* (5th Cir. 2002) 283 F.3d 670.
15. *United States v. Wong* (9th Cir. 2003) 334 F.3d 831.
16. *United States v. Thorn* (8th Cir. 2004) 375 F.3d 679.
17. *People v. Jiang* (Jun. 16, 2005) H026546, opn. ordered nonpub. Sept. 28, 2005.
18. 42 U.S.C. § 12032.
19. *United States v. Gourde* (9th Cir. 2006) 440 F.3d 1065.
20. *United States v. Brooks* (10th Cir. 2005) 427 F.3d 1246.
21. *United States v. Turner* (1st Cir. 1999) 169 F.3d 84.
22. *United States v. Smith* (C.C. Ill. 1998) 27 F.Supp. 2d 1111.
23. *Trulock v. Freeh* (4th Cir. 2001) 275 F.3d 391.
24. *United States v. Lemmons* (7th Cir. 2002) 282 F.3d 920.
25. See also *United States v. Habershaw* (D.Mass. 5/13/02) 2002 WL 33003434.
26. *United States v. Aaron* (6th Cir. 4/3/02) 2002 WL 511557. [Unpublished.]
27. *United States v. Mannion* (4th Cir. 12/19/02) 2002 WL 31839377. [Unpublished.]
28. *United States v. Laine* (1st Cir. 2001) 270 F.3d 71.
29. *United States v. Buckner* (4th Cir. 2007) 473 F.3d 551.
30. *United States v. Carey* (10th Cir. 1999) 172 F.3d 1268.
31. *United States v. Gray* (E.D.Va. 1999) 78 F.Supp. 2d. 524.
32. *Carey*, *supra*.
33. *Gray*, *supra*.
34. *People v. Cochran* (2002) 28 Cal.4th 396, 398–407.
35. *United States v. Katz* (5th Cir. 1999) 178 F.3d 368.
36. *United States v. Upham* (1st Cir. 1999) 168 F.3d 532.
37. *United States v. Tucker* (D.Utah 2001) 150 F.Supp. 2d 1263.
38. *United States v. Simpson* (10th Cir. 1998) 152 F.3d 1241.
39. *People v. Reed* (1996) 53 Cal.App.4th 389.
40. *People v. Imler* (1992) 9 Cal.App.4th 1178.
41. *People v. Jensen* (2003) 114 Cal.App.4th 224.
42. Penal Code § 311.1.
43. *People v. Herman* (2002) 97 Cal.App.4th 1369.
44. See generally, 1 Witkin & Epstein, Cal. Criminal Law: Solicitation—Nature of Crime (2d ed. 1988) § 124, pp. 143–144.
45. *Id.,* Nature of Attempt § 143, p. 161; § 21a.
46. See *People v. La Fontaine* (1978) 79 Cal.App.3d 176*; People v. Adami* (1973) 36 Cal.App.3d 452; but see *People v. Ansaldo* (1998) 60 Cal.App.4th 1190, [when specific intent is present, only slight acts are necessary to show more than mere preparation].
47. These files are quite often named such horrible things, containing what they advertise. It just is what it is, disgusting and invaluable evidence.
48. *United States v. Lacy* (9th Cir. 1997) 119 F.3d 742.

49. Subsections A (Peer to Peer Architectures) and B (Peer to Peer Investigation Techniques) of Section XIII. Peer to Peer File Sharing, were written by Charles W. Barnes and originally published in *Firewall,* Vol. 2, Nos. 3 & 4. These sections have been edited to conform to this manual.
50. *Westerfield v. Superior Court of San Diego County* (2002) 99 Cal.App.4th 994.

Geoff Allard is a deputy district attorney in San Diego County.

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Possession of Child Pornography	311.11(a)	**Wobbler** **M[1] or F 16/2/3** F— If Δ has a prior of this section, then 2/4/6 PC § 290	♦ Knowingly possess or controls any image; ♦ involving a person <18 yr old; ♦ knowing that person is under 18; ♦ image shows person engaged in or simulating "sexual conduct" (*See* PC § 311.4d) (Note: see page 2 of this guide for the definition of "sexual conduct")
Distribution, Importation or the Intent to Distribute Child Porn ***with commercial purpose***[2]	311.2(b)	**F—2/3/6, $100,000** PC § 290	♦ Imports porn for sale or distribution; OR ♦ possess porn with intent to exhibit, exchange or distribute to others ♦ person had knowledge that the image is child porn as defined by PC § 311.4(d) ♦ the act was done for commercial consideration ♦ CALJIC 10.80 ♦ CALCRIM 1141
Distribution, Importation or the Intent to Distribute Child Porn	311.2(c)	**Wobbler** **M or F 16/2/3** F—If Δ has a prior of this section. PC § 290	♦ Imports porn for sale or distribution; OR ♦ possess porn with intent to exhibit, exchange or distribute to others ♦ person had knowledge that the image is child porn as defined by PC § 311.4(d) ♦ the act was done for commercial consideration ♦ CALJIC 10.80 ♦ CALCRIM 1141
Imports or Possess with the Intent to **Distribute to *Children***	311.2(d)	**F—16/2/3, $10,000** PC § 290	♦ Imports into the state any image; OR ♦ possess or duplicates any image ♦ with the intent to distribute the images to an child ♦ person had knowledge that the image is child porn as defined by PC § 311.4(d)
Posing or Modeling of a Child for Child Porn—Commercial Purposes[2]	311.4(b)	**F—3/6/8, $10,000** PC § 290	♦ Person who uses a child, knowing he/she is a child <18 years old ♦ promotes, employs, uses, persuades induces or coerces a child; OR reasonably should have known it was a child ♦ a parent or guardian of a child <18 who is under their control permits that child to ♦ pose or model for any image or live performance of child porn (*See* PC § 311.4(d)) ♦ for commercial purposes.

1 Author: Jeffrey Dort, Deputy District Attorney, San Diego, CA; e-mail *jeff.dort@sdcda.org*; Please email with any changes, errors or suggestions. Version 4.2
M = Misdemeanor, **F** = Felony; **PC § 290** = Penal Code § 290 sex registration required with this section.
2 Commercial purpose does NOT just mean selling, it can mean that the defendant intended to trade the child porn in the future, and thereby use the porn he had to better his collection. "The defendant need only intend to trade the pornography for a commercial purpose at some point in the future". If defendant made the photos and posted them to the Internet with the purpose to trade them he violated PC § 311.4(b). No monetary exchange required. *See People v. Cochran* (2002) 28 Cal.4th 396, 398–407.

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Posing or Modeling of a Child for Child Porn—Non-commercial purposes: aka **Manufacturing Child Pornography**	311.4(c)	**F—16/2/3, $10,000** MANDATORY PRISON (*See* PC § 1203.065(a)) PC § 290	♦ Person who uses a child, knowing he/she is a child <18 years old ♦ promotes, employs, uses, persuades induces or coerces a child; OR reasonably should have known it was a child ♦ a parent or guardian of a child <18 years old who is under their control permits child to ♦ pose or model for any image or live performance of child porn (as defined in 311.4(d))—need NOT prove commercial purposes
Child Pornography Definition SEXUAL CONDUCT DEFINITION as used in the PC § 311 sections	311.4(d)	Definition Section	For a picture to be child pornography, it must depict sexual conduct which is a: ♦ depiction of a person <18 years old, engaged in any conduct including: ♦ intercourse or touching between genital/oral/anal areas; ♦ it may be conduct involving opposite or same sex, or animal; or ♦ penetration of vaginal or rectum; or ♦ masturbation; or ♦ sadism or masochism; or ♦ exhibition of genitals or pubic or rectal area[3]—*if it is exhibition of genitals, it must be for the purpose of sexual stimulation of the viewer; or* ♦ defecation or urination; or ♦ any lewd or lascivious act as defined by PC § 288. ♦ CALJIC 16.194.5 (*See* second paragraph) ♦ CALCRIM 1141—this is the closest CALCRIM to CALJIC 16.194.5 available
Providing Child for Sexual Abuse—Procurement	266j	**F—3/6/8, $15,000** MANDATORY PRISON (*See* PC § 1203.065(a).) PC § 290	♦ Person intentionally transported, provided or made available a child under the age of 16 to another person (or offered the same); ♦ The provider of the child, gave/transported/provided with the specific intent that a lewd or lascivious act be perpetrated upon the child (or offered with the specific intent that a lewd act be committed). ♦ CALJIC 10.72 ♦ CALCRIM 1152

3 *See People v. Spurlock* (2004) 114 Cal.App.4th 1122, 1131 for the "Dost" Factors that can be utilized if you have borderline type pictures, but the defendant has them for child porn purposes. The "Dost" factors look at the characteristics of the photos (scene, people, positions, etc) can be characterized as child pornography.

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Aggravated Sexual Assault of Child	269(a)	**F—15 years to life** PC § 290	♦ A person committed PC § 261(a)2, 264.1, 286 by force[4], 288a by force, 289a; ♦ the victim was under 14 years of age; and ♦ the victim was 7 or more years younger than the perpetrator. ♦ CALJIC 10.55 ♦ CALCRIM 1123
Lewd Act with a Child Under 14	288(a)	**F—3/6/8, $10,000** PC § 290 **Mandatory prison** if Δ used porn to accomplish the act (PC § 1203.066(a)(9); *See also* PC § 1203.066(c).)	♦ Person touched the body of a child[5]; ♦ child was under 14 years of age; and ♦ touching was done with the specific intent to arouse or gratify the lust of the child or the person ♦ CALJIC 10.41 ♦ CALCRIM 1110
Forcible Lewd Act with a Child Under 14	288(b)	**F—3/6/8, $10,000** MANDATORY PRISON per PC § 1203.066(a)1 or (a)9 PC § 290 **Mandatory prison** if Δ used porn accomplish the act (PC § 1203.066(a)(9).)	♦ Person touched the body of a child; ♦ child was under 14 years of age; ♦ touching was done with the specific intent to arouse or gratify the lust of the child or the person; and ♦ touching was done by the use of force, violence, duress, menace, or fear of immediate and unlawful bodily injury on the child or another person. ♦ CALJIC 10.42 (2005 Version) ♦ CALCRIM 1111

4 **Force** means committed by force, violence, duress, menace, or fear of immediate and unlawful bodily injury on the victim or another person. Per PC § 269; and force is "Physical force substantially different from or substantially greater than that necessary to accomplish the lewd act itself." *See People v. Cicero* (1984) 157 Cal.App.3d 465, 474. **NOTE**: if your victim is young, use *People v. Cochran* (2002) 103 Cal.App.4th 8 to argue that **duress** is present using the totality of the circumstances, "When the victim is as young as this victim [age 9] and is molested by her father … in all but the rarest cases duress will be present." *Cochran* at 16. **Duress** has recently been discussed by the California Supreme Court in *People v. Leal* (2004) 33 Cal.4th 999.

5If defendant directs child to touch themselves, this qualifies as a § 288 violation, *see People v. Austin* (1980) 111 Cal.App.3d 110, 114–115; or if child is on the phone and defendant encourages child to touch themselves, this also qualifies as a § 288 violation, *see People v. Imler* (1992) 9 Cal.App.4th 1178, 1181.

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Lewd Act with a Child 14 or 15 Years Old	288(c)	**Wobbler:** **M—1year, $1,000 or** **F—1/2/3** PC § 290	♦ Person touched the body of a child; ♦ child was 14 or 15; and that person was at least 10 years older than the child; ♦ touching was done with the specific intent to arouse or gratify the lust of the child or the person. ♦ CALJIC 10.42.5
Distribution of Child Porn to a Child—*Non-electronic Means* *(if by computer see PC § 288.2(b))*	288.2(a)	**Wobbler** **M—180 days, $1,000 or** **F—16/2/3 $10,000** **2nd Offense—F** *PC § 290—ONLY IF conviction under this section was as a felony*	♦ A person knowingly distributed, sent, exhibited or offered, by any means, including live or recorded telephone message, any harmful matter to a minor; ♦ that person knew that the recipient of the message was a minor (or failed to exercise reasonable care to ascertain the true age of the recipient); ♦ that person did so with the specific intent to arouse or gratify the lust or sexual desires of that person or minor; and ♦ that person also specifically intended to seduce the minor into a physical sexual contact between the person and the minor. ♦ CALJIC 10.58 (2004 Version) and "*harmful matter*" is defined in PC § 313—NOTE: *See* page 7 of this outline for *"harmful matter"* definition. ♦ CALCRIM 1140
Distribution of Child Porn to a Child by *Use of Electronic Means*	288.2(b)	**Wobbler** **M—180 days, $1,000 or** **F—16/2/3 $10,000** **2nd Offense—F** *PC § 290[6] ONLY IF conviction under this section was as a felony*	♦ A person knowingly distributed, sent, exhibited or offered to distribute or exhibited by email, Internet, or other commercial online service, any *harmful matter* to a minor; ♦ that person knew that the recipient of the message was a minor (or failed to exercise reasonable care to ascertain the true age of the recipient); ♦ that person did so with the specific intent to arouse or gratify the lust or sexual desires of that person or minor; and ♦ that person also specifically intended to seduce the minor into a physical sexual contact between the person and the minor. ♦ CALJIC 10.58 (2004 Version) and "*harmful matter*" is defined in PC § 313—NOTE: *See* page 7 of this outline for *"harmful matter"* definition. ♦ CALCRIM 1140

6 HOWEVER, if there is no PC § 290 requirement, you can still use PC § 290(a)(2)(E) to argue to the sentencing judge that a court can order PC § 290 registration if the crime was sexually motivated and make sure the court makes a finding on the record that "the person committed the offense as a result of sexual compulsion or for the purposes of sexual gratification."

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Luring—Arranging a Meeting with a Child	288.3	**M—if meeting set; F—16/2/3 if meeting set and Δ shows up at the meeting** **F—2/3/4 if Δ is a PC § 290 registrant** PC § 290	♦ Person arranges a meeting with a minor, or someone they think is a minor; ♦ person was motivated by an abnormal interest in children; ♦ person did this for the purpose of a PC § 288 or to expose him or herself or to have the child expose him or herself.
Continuous Sexual Abuse of a Child	288.5	**F—6/12/16** PC § 290	♦ A person who resided with the child or had re-occurring access to the child; ♦ engaged in three or more acts of PC § 288 conduct or three acts of substantial sexual conduct as described in 1203.066, with a child less than 14 years old; ♦ these acts occurred over a period of time not less than three months in duration; ♦ CALJIC 10.42.6 ♦ CALCRIM 1120
Sexual Intercourse with a Child	288.7(a)	**25 to life** PC § 290	♦ Person had sexual intercourse or sodomy with a child ♦ child was 10 years or younger
Oral Copulation or Sexual Penetration of a Child	288.7(b)	**15 to life** PC § 290	♦ Person engages in oral copulation or sexual penetration with a child ♦ child was 10 years or younger
Annoy or Molest of a Child (<18)	647.6(a)	**M—1year, $1,000 F—16/2/3 if prior this section; or F—2/4/6 if prior F this section or PC § 288, 311.4** PC § 290	♦ A person engaged in acts or conduct directed at a child under 18 which would unhesitatingly disturb or irritate a normal person if directed at that person; and ♦ the acts or conduct were motivated by an unnatural or abnormal sexual interest in the victim. ♦ CALJIC 16.440 ♦ CALCRIM 1122

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Secretly Photographing Another aka Up-skirting	647(k)2	**M—180 days, $1,000** NO PC § 290[7]	♦ Any person who uses any concealed camera or recording device to secretly photograph anyone; ♦ under or through their clothing ♦ for the purpose of viewing the body or undergarments of the person without their consent ♦ invading their privacy where they have a reasonable expectation of privacy ♦ with the intent to arose or gratify the lust or desires of the defendant
Secretly Photographing Another—While Changing aka Bathroom-cam	647(k)3	**M—180 days, $1,000** NO PC § 290[8]	♦ Any person who uses any concealed camera or recording device to secretly photograph anyone; ♦ under or through their clothing ♦ for the purpose of viewing the body or undergarments of the person without their consent ♦ and invading their privacy in which they have a reasonable expectation of privacy ♦ while that person was in a bathroom, bedroom, changing room or other room where that person would have a reasonable expectation of privacy
Solicitation to Commit Sex Crime	653f(c)	**F—2/3/4** PC § 290	♦ Person solicited another to commit PC § 261(a)2, 289, 288(a)(c), 264.1 or 288; ♦ at the time of the solicitation, the solicitor had the specific intent that the crime above would be committed; ♦ the soliciting message was received by the intended recipient/solicitee. ♦ CALJIC 6.35 ♦ CALCRIM 441
Advertising for Child Pornography or Obscene Material	311.10	**Wobbler** **M—180 day $1,000;** **F—2/3/4** PC § 290	♦ Person advertising for sale or distribution any obscene matter ♦ person had knowledge that the image is child porn as defined by PC § 311.4(d)

7 HOWEVER, if defendant is convicted of a non-§ 290 crime, you can use PC § 290(a)(2)(E) to argue to the sentencing judge that a court can order PC § 290 registration if the crime was sexually motivated, and make sure court makes a finding on the record that "the person committed the offense as a result of sexual compulsion or for purposes of sexual gratification."

8 HOWEVER, if defendant is convicted of a non-290 crime, you can use PC § 290(a)(2)(E) to argue to the sentencing judge that a court can order PC § 290 registration if the crime was sexually motivated, and make sure court makes a finding on the record that "the person committed the offense as a result of sexual compulsion or for purposes of sexual gratification."

2007 CALIFORNIA CHILD PORNOGRAPHY AND CHILD ABUSE CHARGING MATRIX[1]

Crime Title	Penal Code Section	Punishment	Elements and CALJIC and/or CALCRIM # if They Exist
Defenses to Porn Charges	311.8	Definition Section Only	It "shall be a defense to a violation of this chapter (PC § 311–312)" if: ♦ the act was done in aid of legitimate scientific purposes ♦ the act was done in aid of legitimate educational purposes If the act was sending porn to a child, it shall be a defense if the defendant restricted access of the porn by reasonably ascertaining that the person was 18 years or older or using a credit card.
Harmful Matter and Matter Defined	313(a)	Definition Section	"Harmful matter" is anything that: ♦ taken as a whole, applying contemporary statewide standards ♦ appeals to the prurient interest, and ♦ depicts or describes in a patently offensive way sexual conduct, ♦ matter lacks serious literary, artistic, political, or scientific value for minors. ♦ CALJIC 10.58 (Third paragraph) "Matter" is: ♦ any book, magazine, newspaper, or other printed or written material, or any picture, drawing, photograph, motion picture, or other pictorial representation, or any statute or other figure or any recording transcription or mechanical, chemical or electrical reproduction or any other articles, equipment, machines or materials. It also means live or recorded telephone messages when transmitted, disseminated, or distributed as part of a commercial transaction. ♦ CALJIC 16.183

This page intentionally left blank.

Appendix B

Possession of Child Pornography Special Instruction

Every person who knowingly possesses or controls any matter, representation of information, data, or image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disc, data storage media, CD-ROM, or computer-generated equipment or any other computer-generated image that contains or incorporates in any manner, any film or filmstrip, the production of which involves the use of a person under the age of 18 years, knowing that the matter depicts a person under the age of 18 years personally engaging in or simulating sexual conduct, is guilty of the crime of Possession of Child Pornography.

"Sexual conduct" means any of the following, whether actual or simulated: sexual intercourse, oral copulation, anal intercourse, anal oral copulation, masturbation, bestiality, sexual sadism, sexual masochism, penetration of the vagina or rectum by any object in a lewd or lascivious manner, exhibition of the genitals or pubic or rectal area for the purpose of sexual stimulation of the viewer, any lewd or lascivious sexual act as defined in Section 288, or excretory functions performed in a lewd or lascivious manner, whether or not any of the above conduct is performed alone or between members of the same or opposite sex or between humans and animals. An act is simulated when it gives the appearance of being sexual conduct.

Two or more people may possess something at the same time.

A person does not have to actually hold or touch something, to possess it. It is enough if the person has control over it or the right to control it), either personally or through another person.

In order to prove the above crime, the following elements must be shown:

1. A person knowingly possessed child pornography as described above.
2. That person knew the matter depicted a child under the age of 18 years.

Special Instruction, from California Penal Code sections 311.11 and 311.4.

This page intentionally left blank.

Appendix C

Computer Forensics Expert Questions

RCFL *San Diego* **Sample questions for court testimony** **Updated 3/6/2006**

Regional Computer Forensics Lab

General Questions

(Examiner, CFE, RCFL, imaging and examination process)

Mr. Hamon, can you please state your name and occupation?

My name is Tim Hamon. My official title is "IT Specialist, Computer Forensic Examiner" with the Federal Bureau of Investigation. I currently work as a CFE for the FBI and I'm assigned to the San Diego Regional Computer Forensics Laboratory.

What does a CFE do?

The short answer is that a CFE is a bridge between the technical aspects of computer evidence and the investigator. I take questions from an investigator and try to find information on the computer evidence to answer those questions. Once I determine the answer to the questions, I write a report that tries to explain what those answers are, and if necessary, what those answers mean. I am a geek-to-English translator.

What about the RCFL? What is that?

The RCFL is essentially a task force of various local, state and federal agencies in the San Diego area. It is a cooperative organization that provides computer forensic services to San Diego and Imperial counties. The lab is composed of nearly twenty CFEs from different agencies and organizations. To this end, I work with people from the SDPD, the Sheriff's office, the CHP, the DEA, the Border Patrol and several other agencies.

The principle behind the RCFL, the one in San Diego or any of the other ones around the country, is that the power of the whole is more powerful than the sum of its parts. The RCFL can do more than several agencies working independently. Thus, the RCFL can conduct "forensic business" in cases that would be impossible or impractical for an independent agency to do by itself.

Can you describe your work history in the context of law enforcement?

I joined the US Border Patrol in 1998. I worked as a patrol agent, out in the field, for the Brown Field station in San Diego until October of 2001. In late October of that year, I was assigned to the RCFL. I later switched agencies and joined the FBI as a CFE in April of 2003.

Can you describe your educational background?

I graduated from UCSD 1997 with a bachelor's degree in writing. I graduated from National University in 2002 with a master's degree in Software engineering.

Can you summarize your training in the context of computers and your work with the RCFL?

I have received over 900 hours of specialized training during my time at the RCFL. This training covers a great deal of ground. The CFE training curriculum covers many general things about computers, as well as some specific things. In general, we learn about operating systems (such as the various flavors of Windows and Linux), computer hardware and networking operations. Specifically, we learn about the way data is stored on a computer and how that data can be recovered and put into a format that can be understood. Much of this training is on the tools that we use for that task.

Can you describe the work you do, in general terms, at the RCFL?

I do two things, primarily. I perform forensic examinations and I conduct research.

Occasionally, I conduct research. I test hardware and software that are significant to the computer forensic community. There are times when new hardware or software is released and the RCFL is interested in what

Examiner:	I.D. #:	Approved By:	Date of Report:
CFE Hamon	**023**		**3/6/2006**

that tool can do. I will design a series of tests, conduct the tests and write a paper based on the results. The RCFL will then determine if that new tool is suitable for use and if so, in what capacity.

More than 95% of my time is spent conducting forensic examinations. For the forensic examinations, I touched on that briefly, earlier. I am a geek-to-English translator. There is a lot of data on, say, a computer's hard drive. My job is to make meaningful, significant determinations about that data and explain what it is and what it means.

In some cases, the data is there and it speaks for itself. My job is simply to recover it and provide it to the case agent in a way that makes sense to the average person. In some cases, it is more important to determine how that data got there in the first place or even why specific data wasn't there.

In almost every case, the investigator wants to know how the computer evidence is related to the crime he is investigating. My job is to find if and how that computer is related and then describe that relation.

Can you describe the process for us?
The process begins before anything is ever submitted to the RCFL. An investigator comes across computer evidence via a search warrant or with the owner's consent. The computer evidence goes through that agency's chain of custody and makes its way over to the RCFL. Along with the computer evidence, the investigator submits what is called a "request for service." This form contains administrative information, such as the investigators' name and agency, as well as the details of the case.

What kind of details?
It depends, although there are some standard things that go on or accompany the service request. The point of the SR, however, is for the investigator to describe what he thinks will be on the computer, with regard to the crime that he is investigating.

So the computer evidence and the service request have been submitted. What is next?
The case gets assigned to a CFE. Using myself as an example, I would get a file that contains the SR. When I got to the case, I would go through what we call the "imaging" process.

Can you describe what imaging is?
In the simplest terms, we are copying the data from the original evidence, such as a computer's hard drive, floppy disk or CD. It is more complex than simply using windows to "drag and drop" files from one place to another, but the principle is the same. We are taking the data from the original evidence and placing it on media (like a hard drive). Commonly, people refer to this as "cloning" or "duplicating" the original evidence, but terms can mean different things, depending on who you ask. We refer to imaging as "an accurate representation of the data found on the original source."

Why would you image something?
It is a way of safe-guarding the original evidence. This allows for us to have more than one copy of the original evidence, in case it were to become damaged or otherwise altered. Also, it allows for a better process. The computer evidence can be imaged and the original evidence can be returned to its owner while the rest of the forensic process is completed. Since it can take months to complete the examination, this is the most reasonable method to get the evidence back to the investigator, who will maintain it or release it back to the owner.

After you image the evidence, what comes next?
The "exam" portion follows the imaging. During this phase, the CFE is doing his best to answer the questions posed by the investigator. Using the service request, the affidavit, the warrant and by speaking to the investigator, the CFE is using his training and experience to answer those questions.

Why don't you just provide the investigator with an image of the evidence?
In some rare cases, we do. Usually real problem is that the investigator may not have the tools, training, equipment, experience and education to do the exam.

Regional Computer Forensics Lab

Once you collect an idea of the case, what do you do?

This is where the science of the computer person meets the intuition of an investigator. Some times, the questions that the investigator asks can be answered by recovering files. These can be web pages, pictures, MS Word documents or other files that are created or managed by the user. In such a case, the CFE's job is to simply recover the files and present them in a way that can be used by the investigator, such as printing out relevant pictures or emails or placing relevant movies on a CD.

Sometimes, the CFE must do more than recover files. The CFE is often required to investigate the Windows registry, recover deleted or lost files, analyze data fragments and piece together pieces of a puzzle to explain why things exist the way they do. Again, all of this is an attempt to ask the questions that the investigator asks on the service request.

Examiner:	I.D. #:	Approved By:	Date of Report:
CFE Hamon	**023**		**3/6/2006**

This page intentionally left blank.

Appendix D

Sample Forfeiture Order

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF

THE PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, v. CHESTER J. MOLESTER, Defendant.	**COURT NO.** **ORDER**

Per Penal Code section 312 and Penal Code section 502.01(c), which declares that in a forfeiture action against computers used in the sexual exploitation of children, "(n)o person shall hold a valid interest in the property if, by a preponderance of the evidence, the prosecuting agency shows that the person knew or should have known that the property was being used in violation of, or conspiracy to commit a violation of, Section 288(a)…311.1, 311.2, 311.3, 311.4, 311.5, 311.10, (or) 311.11…" The defendant having pleaded guilty to xxx counts of Penal Code section and further having stipulated to the forfeiture of the computers used in this/these crime(s), the court hereby orders that the computers seized by INSERT AGENCY, their software, data, and all associated licenses, be forfeited to the prosecuting agency per Penal Code section 502.01(c).

Dated: March 20, 2007

_____
Judge of the Superior Court

This page intentionally left blank.