

# COMPUTER FORENSICS 101: HOW TO SOUND LIKE A GEEK (WITHOUT BECOMING ONE)

The Federal Judicial Center  
Judicial Education Center  
*Orientation Seminar for Assistant Federal Defenders*  
November 12-16, 2007  
Santa Fe, New Mexico

Steven Kalar  
Senior Litigator, N.D. Cal. FPD

Sumter Camp  
Supervisory AFD, Middle D. Tenn. FPD

---

---

Science is supposedly the method by which we stand on the shoulders of those who came before us. In computer science, we all are standing on each others' feet.

— G. Popek.

Artificial Intelligence usually beats natural stupidity.

— Anonymous

Computers are like Old Testament gods; lots of rules and no mercy.

— Joseph Campbell

After growing wildly for years, the field of computing appears to be reaching its infancy.

— John Pierce

---

---

## Table of Contents

I.	Introduction: .....	1
II.	Possession of Child Pornography: .....	2
	A.    The Possession Statute - 18 USC § 2252A(a)(5)(B) .....	2
	B.    The “Internet Cache” and Straight “Possession” Cases .....	2
	C.    Location, Location, Location .....	5
III.	“Receipt” of Child Pornography: .....	6
	A.    The Receipt Statute - 18 USC § 2252A(a)(2) .....	6
	B.    Possession = Receipt .....	6
	C.    No Double-Jeopardy Bar for “Possession” Plea, then “Receipt” Prosecution .....	7
	D.    “Distribution” Charges and Peer-to-Peer Networks .....	7
IV.	Transportation of Child Pornography: .....	8
	A.    The Transportation Statute - 18 USC § 2252A(a)(1) .....	9
	B.    Good guideline twist for transportation cases: .....	9
	C.    File Time Stamps: Creation Dates, Modified Dates, and Defenses .....	10
V.	Production of Child Pornography: .....	11
	A.    Child Porn Production Statute - 18 USC § 2251 .....	11
	B.    Beware of Cross-References: .....	11
	C.    Large Files are Red Flags for Production of Child Porn .....	12
VI.	Miscellaneous Forensic Pointers .....	13
	A.    Larger Internal and External Hard Drives Increase Dangers in Sex Crime Cases .....	13
	B.    Tales from the Crypt .....	16
	C.    Search Issues (Spam, Spam, Spam) .....	17
	D.    OMG, ICQ! (LOL) .....	18
	E.    Gadgets will Get You (Cell Phones, Palms, Treos, Blackberries) .....	19
	F.    Cheapskate Forensic Review .....	20

**I. Introduction:** The Adam Walsh Act<sup>1</sup> and the frenzy of national interest in child porn and sex crime prosecutions has made these types of cases an increasingly large part of federal dockets. These cases present a number of challenges for the defense bar: clients with no criminal records and no experience with the criminal justice system, extremely unsympathetic facts, and extraordinarily high sentencing exposures.

One of most challenging aspects of these cases is that they inevitably involve computers and digital evidence. Moreover, much depends on extremely technical aspects of this evidence – were images found in the internet cache or unallocated space? Were e-mails (with child porn attachments) solicited or downloaded to the computer unwittingly? Is a particular image produced by the client, or downloaded off the internet?

This outline and presentation gives an overview of some of the most dangerous aspects of federal sex crimes prosecutions, and then provides an introduction to forensic principles relating to each of these legal issues. While this is not a comprehensive review, we hope that these materials establish a starting point for counsel and their clients to discuss forensic evidence in sex crime cases. We also encourage counsel to use and review this outline with their forensic examiners, to help sharpen their review of seized computer and digital evidence.

The outline is organized by laying out some of the most common federal statutes used in sex crime prosecutions. We then define some of the key forensic terms that frequently arise in these types of prosecutions. Finally, for each type of offense, we will identify common forensic issues and possible defenses or sentencing mitigation tactics.

We welcome any insights, comments, or corrections relating to these materials, and hope that you find this information helpful in defending the newest – and most challenging – category of federal crimes.

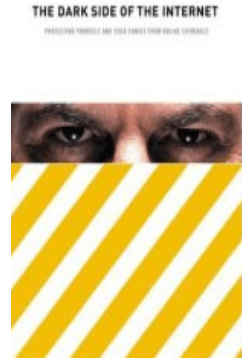
Steven Kalar  
Senior Litigator  
Northern District of California  
Federal Public Defender  
Steven\_Kalar@fd.org

Sumter Camp  
Senior Litigator  
Middle District of Tennessee  
Federal Public Defender  
Sumter\_Camp@fd.org

---

<sup>1</sup> The Adam Walsh Child Protection and Safety Act, Pub. L. 109-248 (2006).

**II. Possession of Child Pornography:** The most common federal sex crime offense is “straight” possession of child pornography. Unless a client has a prior sex crime offense, this crime carries no mandatory minimum sentence – making it a (comparatively) attractive alternative to other mandatory-minimum crimes, such as “receipt” or “transportation” of child pornography. Nonetheless, the federal sentencing guidelines for straight possession can be unbelievably high. After the Adam Walsh Act (and amendments to the Sentencing Guidelines from the PROTECT Act<sup>2</sup>), straight possession cases can easily carry a guideline range well in excess of five years<sup>3</sup> – even for defendants in Criminal History Category I.



**A. The Possession Statute - 18 USC § 2252A(a)(5)(B)**

1. Any person who “knowingly possesses any . . . material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer;” 18 USC § 2252A(a)(5)(B).
  - a. “[S]hall be fined under this title or imprisoned not more than 10 years, or both, but, if such person has a prior conviction [for various sex offenses] such person shall be fined under this title and imprisoned for not less than 10 years nor more than 20 years.” 18 USC § 2252(A)(b)(2).

**B. The “Internet Cache” and Straight “Possession” Cases:** A frequent issue in straight-possession cases is whether *all* images recovered from a computer should count to establish criminal liability, or higher sentencing exposure. One specific directory on defendants’ computers has been the subject of much litigation – the “internet cache.”

The “internet cache” is the name of a directory within a computer’s operating system,

---

<sup>2</sup> Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (“PROTECT Act”), 2003.

<sup>3</sup> The base offense level for straight possession is 18. USSG § 2G2.2(a)(1) (Nov. 1, 2006). If there are images of prepubescent minors, there is a two-level specific offense adjustment. *Id.* § 2G2.2(b)(2). Sadistic or masochistic images trigger an additional four-level specific offense adjustment. *Id.* § 2G2.2(b)(4). Use of computer is another two-level increase. *Id.* § 2G2.2(b)(6). There is then an increase for the number of images – for example, over six hundred images is a five-level specific offense adjustment. *Id.* § 2G2.2(b)(7)(D). Note also that videos count as (at least) seventy-five images apiece. *Id.*, comment. n. 4(B)(ii).

If all of the above adjustments apply (and they frequently do) a typical straight-possession defendant will be at Criminal History I, Offense Level 31 after trial, or CH I, OL 29 with a timely plea and acceptance of responsibility. In other words, with a timely plea the defendant in this example will be looking at 87-108 months in custody.

where images and material from the internet are temporarily stored.<sup>4</sup> Here is a good definition of “internet cache:”

What is the Internet Cache? Your Internet cache is in the Temporary Internet Files folder on your hard disk. This is where Web pages and files (such as graphics) are stored as you view them. This speeds up the display of pages you frequently visit or have already seen, because it is faster to open them from your hard disk than from the Web. The downside of this is that it takes up space on your hard disk, and it can sometime cause problems in loading a page that you have visited many times before.

<http://www.shepherd.edu/compserv/prevent/internetch.htm> (visited May 5, 2007).

The Ninth Circuit has defined a “cache” as follows:

---

<sup>4</sup> The precise location of the internet cache depends on the computer’s operating system, and the internet browser used. For example, for the Firefox browser the cache may be located here: C:\Documents and Settings\[USER]\Local Settings\Application Data\Mozilla\Firefox\Profiles\wnkt3v3e.default\Cache . The Firefox cache can be viewed by simply typing “about:cache” in the browser’s address bar.

For Microsoft’s Internet Explorer browser, by contrast, the cache may be found by doing the following (this procedure works for IE 7):

1. Open Microsoft Internet Explorer.
2. Open the Tools menu and choose “Internet Options.” A new window titled “Internet Properties” appears.
3. In the Browsing History section of the Internet Options window, click the “Settings” button. A box titled, “Temporary Internet Files and History Settings” appears.
4. In this box, click the “View Files” button. After a brief delay, a new Windows Explorer window appears. This window displays all of the Temporary Internet Files stored on the computer and their location on the local hard drive. The window also displays the URL where each temporary file came from.
5. You can copy files displayed in this window, view them, and save them to another location (an option that caused the defendant problems in the *Romm*, case, *supra*).

A cache is “a computer memory with very short access time used for storage of frequently or recently used instructions or data.” MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY 171 (11th ed.2003). “[I]nformation is cached by placing it closer to the user or user application in order to make it more readily and speedily available....” NEWTON’S TELECOM DICTIONARY 189 (22nd ed.2006).

*United States v. Ziegler*, 474 F.3d 1184, 1185 n.3 (9th Cir. 2007).

Can one be criminally liable for straight possession of child pornography, for images recovered from the internet cache of a computer? Yes – at least, in the Ninth Circuit.

In *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006), the Ninth Circuit considered a challenge to a conviction for possession of more than three images of child pornography, when the images were found in the defendant’s internet cache. The Court concluded that – based on the evidence in the case – the conviction would stand:

In short, we hold there was sufficient evidence for the jury to conclude that the images in the cache were “visual depictions” because they could be accessed and viewed by Romm. Further, given Romm’s ability to control the images while they were displayed on screen, and the forensic and *other evidence that he actually exercised this control over them*, there was sufficient evidence to support the jury’s finding that Romm possessed three or more images of child pornography. Coupled with Romm’s conceded knowledge that the images were saved to his disk, the prosecution produced sufficient evidence to establish every element of knowingly possessing child pornography under 18 U.S.C. § 2252A.”

*Id.* at 1000-01 (emphasis added). An important aspect of *Romm* – and a subject of focus for defense forensic examiners – is the defendant’s access to and manipulation of images within the cache.

The importance of *active* access to these internet cache files is illustrated by another Ninth Circuit case, *United States v. Kuchinski*, 469 F.3d 853, 861-62 (9th Cir. 2006). In *Kuchinski*, the Court explained that, *for purposes of sentencing*, the number of images in the defendant’s internet cache could not be used to increase a defendant’s sentencing range under the guidelines. *Id.* at 861-62 (“The difference is wholly related to the cache files. Did Kuchinski knowingly receive and possess the images in those files, or, rather, does the evidence support a determination that he did? We think not.”) (footnote omitted).<sup>5</sup> The Court in *Kuchinski* noted that a web browser will download files into the internet cache automatically, and often without the user knowing it is happening:

---

<sup>5</sup> Unfortunately, evidence that a defendant viewed and exercised control over images in the internet cache can be enough to support a conviction. *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006); *see also* <http://circuit9.blogspot.com/2006/07/case-o-week-ram-rom-wrong-ninths.html>. In *Romm*, however, the defendant admitted to exerting (some) level of control over the images stored in the internet cache. That may be a factual distinction that can be teased into a defense at trial.

According to the evidence before the district court, when a person accesses a web page, his web browser will automatically download that page into his Active Temporary Internet Files, so that when the site is revisited the information will come up much more quickly than it would have if it had not been stored on the computer's own hard drive. When the Active Temporary Internet Files get too full, they spill excess saved information into the Deleted Temporary Internet Files. All of this goes on without any action (or even knowledge) of the computer user. A sophisticated user might know all of that, and might even access the files. But, "most sophisticated-or unsophisticated users don't even know they're on their computers."

*Id.* at 862.

Both *Romm* and *Kuchinski* involved child porn images located in a defendant's internet cache. The different outcomes in those two cases turned on evidence bearing on the defendant's *knowing access and control* of those images. Obviously, in internet cache cases, forensic analysis of access history of child porn images should be a top priority.

### C. Location, Location, Location

It is common for the government to provide electronic discovery in the form of HTML ("web") files generated from forensic software. That list may, for example, contain images with a long print-out of the file name and folder location.

That "summary" discovery report is often woefully insufficient because it fails to give intelligible data about the true location of the file.

The same file can have radically different evidentiary significance when it is located in different areas of a computer hard drive. For example, pictures of nude children at the beach (taken by the client) may be innocuous (or at least, not criminal) when stored in a folder that contains many other vacation pictures. That same beach picture, however, can have a very different significance when it is stored in a folder containing images of undisputed child pornography. The context provided by the *location* of the file – and the nature of other files in a folder – may have real evidentiary weight on whether the beach image is pornographic, or not.<sup>6</sup> Put differently, when non-sexual nude pictures of children – taken by the client – are stored in a folder that contains child porn copied off of the web it raises the real danger of porn *production* charges.

Hence, the *location and context* of a file is critical information for defense counsel. The problem is that, for a variety of reasons, folder (and hence, location) names are often not intuitive. For example, file-servers, use-group dumps, and digital camera software will often set

---

<sup>6</sup> Even if the *location* of client-generated images of nude children is somehow excluded from trial, the prosecutor's knowledge of how the client categorized those images will not help plea discussions. The logic of context is damning: the *defendant* considered nude images of children to be erotic, because he stored them in a folder dedicated to child pornography material.

up long, numeric, and non-descriptive folder names for files. These important folders will often be obscured by layers of higher directories. **Therefore, lawyers who work with forensic experts should ask for general descriptions about where problem files are located, and for a description of other files are located around problem evidence in those folders.**

**III. “Receipt” of Child Pornography:** The “receipt” of child pornography is a particularly frustrating aspect of a generally frustrating area of law. Section 2252A makes it a crime to “receive” child pornography – and that crime is far more serious than straight possession of child porn. First, “receipt” carries a five year mandatory minimum sentence (and more if the defendant has a sex offense prior). Second, the guidelines are considerably higher for “receipt” cases. Under USSG § 2G2.2(a)(1), the *base* offense level for a receipt case is



**BitTorrent, a leading peer-to-peer (P2P) file sharing communications protocol**

twenty-two – *four levels higher* than the base offense level for straight possession. *See* USSG § 2G2.2(a)(2) (Nov. 1, 2006). Finally, these greater penalties are – as a practical matter – potentially at risk in every child pornography case. As will be described below, while courts acknowledge that there is no practical difference between possession and receipt cases, they have been unwilling to find that the receipt statute is duplicative or vague.

**A. The Receipt Statute - 18 USC § 2252A(a)(2):**

1. “Any person who . . . knowingly receives or distributes . . . any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer . . .” 18 USC § 2252A(a)(2).
  - a. “[S]hall be fined under this title and imprisoned not less than 5 years and not more than 20 years, but, if such person has a prior conviction [for various sex offenses] such person shall be fined under this title and imprisoned for not less than 15 years nor more than 40 years.” 18 USC § 2252(A)(b)(1)

**B. Possession = Receipt:** As noted above, the Ninth Circuit has been unwilling to parse out the differences between possession, and the (more-dangerous) receipt charge. This is best illustrated in a discussion from the *Romm* decision:

Since Romm knowingly possessed the files in the internet cache, *it follows that he also knowingly received them*. Federal law makes it a crime to “knowingly receiv[e] or distribut[e] ... any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce...” 18 U.S.C. § 2252A(a)(2). Generally, federal statutes criminalizing the receipt of contraband require a “knowing acceptance or taking of possession” of the prohibited item. . . . Moreover, we have applied this principle to 18 U.S.C. § 2252’s prohibitions on receiving and possessing child

pornography. See *Mohrbacher*, 182 F.3d at 1048 (“An individual who ... takes possession or accepts delivery of the visual image . . . has therefore certainly received it.”). Specifically, in *Mohrbacher*, we held that downloading child pornography constitutes both the act of possession and receipt. *Id.* Here, we have held that the files stored to the cache were possessed by Romm, and thus, that the caching of files, on the facts of this case, is analogous to downloading for the purpose of possession. By analogy, it follows under *Mohrbacher* that knowingly taking possession of the files in the cache also constitutes the “knowing receipt” of those files. Therefore, we hold that the evidence was sufficient to sustain Romm’s conviction for receiving child pornography.

*Romm*, 455 F.3d at 1001 (emphasis added) (internal citations omitted).

**C. No Double-Jeopardy Bar for “Possession” Plea, then “Receipt” Prosecution:**

“Possession” and “receipt” of child pornography are so intertwined that surely conviction of the former must raise a double-jeopardy bar to prosecution of the latter? No so, in the Ninth Circuit. In *Kuchinski*, a conditional [11(c)(1)(C)] plea to straight possession went sideways. The government then went forward on “receipt” charges. The defendant (persuasively) argued that the receipt prosecution was barred by double jeopardy. The Ninth disagreed, and held that because receipt was a “greater offense,” there was no double-jeopardy bar to a trial on that charge. *Kuchinski*, 469 F.3d at 859.

**D. “Distribution” Charges and Peer-to-Peer Networks:** Section 2252A(a)(2) of Title 18 also provides the five-year mandatory minimum – and the extraordinarily high guidelines – for *distribution* of child pornography. 18 USC§ 2252A(a)(2). Frequently, however, “distribution” charges can be triggered by almost-inadvertent use of “peer-to-peer” software on a defendant’s computer.



“Peer to Peer” or “P2P” is a giant computer network among users on the internet, designed to locate and share files. The recent brouhaha over copyrighted song and video sharing on the internet involves users who are on peer-to-peer networks. These networks are often used to share child pornography as well. There are many software programs designed to allow users easy access to P2P networks: Napster (or at least, the old Napster), Kazaa, Limewire, BitTorrent, and Morpheus are among the most popular.

All of these programs encourage *sharing*. In other words, the network is more fruitful and productive if users don’t just download files from other computers. Instead, this software wants users to allow other computers access to stored files within their drives.

As a result, the default setting for this software allows uploading of files from a special folder within the user’s computer. If a user does *not* allow access to his own “shared” folder for

uploading, his own downloading rights are restricted or limited.<sup>7</sup> For illegal song sharing, this means that a user's copy of "Saturday Night Live" that is stored on his computer will be accessible to others on the network to upload. The same analogy holds true for child pornography.

Unfortunately, allowing others on a P2P network access to child pornography in a "shared" folder triggers criminal liability for the distribution of pornography. *See, e.g., United States v. Shaffer*, 472 F.3d 1219, 1224 (10th Cir. 2007) ("We have little difficulty in concluding that Mr. Shaffer distributed child pornography in the sense of having 'delivered,' 'transferred,' 'dispersed,' or 'dispensed' it to others. He may not have actively pushed pornography on Kazaa users, but he freely allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those items.")

There may be a case where a child porn defendant had absolutely no idea that images were being uploaded from his computer via a P2P network. We've yet to encounter that case – generally, clients are uncomfortable with this aspect of the software, but don't know how to (or don't want to) disable the uploading feature. Therefore, beware of the danger of *distribution* charges in child porn cases that involve peer-to-peer networks.

**IV. Transportation of Child Pornography:** Like "receipt," the "transportation" of child pornography can be a very frustrating charge because the transportation involved is often only incidental to the possession of the images. For example, in districts with international airports it is not uncommon for defendants to be



---

<sup>7</sup> For example, here is a discussion for the "BitTorrent" help pages:

Question: Can I stop the BitTorrent client from uploading?

Answer: You can minimize the amount of bandwidth used for uploading in the program settings, but not stop it. If you are concerned about bandwidth usage, don't be--BitTorrent uses very little bandwidth to send small pieces of the file at a time.

It is well known BitTorrent downloaders engage in tit-for-tat with their peers. In order for everyone to have the best downloading experience, you have to share what you get. Some peers will not send file pieces to clients that send nothing up in return, making for a very slow download. But if you decide you can't share a torrent, you can either take it out of your queue (by selecting it and clicking on the red Remove button). Taking it out of your queue is not the same as deleting it from your computer.

[http://support.bittorrent.com/cgi-bin/bittorrent.cfg/php/enduser/std\\_adp.php?p\\_faqid=11&p\\_created=1149634710&p\\_sid=pixWfgOi&p\\_accessibility=0&p\\_redirect=&p\\_lva=&p\\_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD0yMTAmcF9wcm9kcz0mcF9jYXRzPSZwX3B2PSZwX2N2PSZwX3NlYXJjaF90eXBIPWFuc3dlcnMuc2VhemNoX25sJnBfcGFnZT0x&p\\_li=&p\\_topview=1](http://support.bittorrent.com/cgi-bin/bittorrent.cfg/php/enduser/std_adp.php?p_faqid=11&p_created=1149634710&p_sid=pixWfgOi&p_accessibility=0&p_redirect=&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD0yMTAmcF9wcm9kcz0mcF9jYXRzPSZwX3B2PSZwX2N2PSZwX3NlYXJjaF90eXBIPWFuc3dlcnMuc2VhemNoX25sJnBfcGFnZT0x&p_li=&p_topview=1)

arrested coming off of airplanes with laptops full of child porn.<sup>8</sup> While these defendants often carried their laptop only as part of their own possession of the porn, as a technical matter they are also guilty of “transportation” of the pornography.

#### A. The Transportation Statute - 18 USC § 2252A(a)(1)

1. “Any person who – knowingly . . . transports . . . in interstate or foreign commerce by any means, including by computer, any child pornography. . . .” 18 USC § 2252A(a)(1).
  - a. “[S]hall be fined under this title and imprisoned **not less than 5 years** and not more than 20 years, but, if such person has a prior conviction [for various sex offenses] such person shall be fined under this title and imprisoned for **not less than 15 years** nor more than 40 years.” 18 USC § 2252A(b)(1) (emphasis added).

**B. Good guideline twist for transportation cases:** In a complicated - but welcome - quirk in the guidelines, there is a way to help mitigate the high base offense levels for transportation cases. As shown below, Guideline § 2G2.2 permits a reduction when there was no intent to traffic or distribute child porn:

##### (a) Base Offense Level:

(1) 18, if the defendant is convicted of 18 U.S.C. § 1466A(b), § 2252(a)(4) [*sells, or possesses with intent to sell child porn*], or § 2252A(a)(5) [*possesses child porn*].

(2) 22, otherwise [*for example, § 2252A(a)(1) – transports child porn – or (a)(2) – receives or distributes child porn*].

##### (b) Specific Offense Characteristics

(1) If (A) subsection (a)(2) applies; (B) the defendant’s conduct was limited to the

---

<sup>8</sup> For an example of this type of search, *see United States v. Arnold*, 454 F.Supp.2d 999 (C.D. Cal. 2006). *Arnold* is a typical border search of digital media at an international airport. It is atypical, however, because district judge Dean Pregerson suppressed child pornography on this media – finding that this was an unlawful search. *Id.* at 1006 (“In every Fourth Amendment case, the Court must consider the circumstances of the search without the benefit of hindsight. The fact that the officers’ search uncovered what they believe to be child pornography does not transform what was at best a hunch into the reasonable suspicion necessary for an invasive search. ‘[A] search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from its success.’ *United States v. Di Re*, 332 U.S. 581, 595, 68 S. Ct. 222, 92 L.Ed. 210 (1948). Thus, to justify its intrusive search, the government must show that the search was based on an articulable reasonable suspicion that Arnold was carrying contraband in his laptop computer. For the foregoing reasons, the government has not met its burden in this case.”)

receipt or solicitation of material involving the sexual exploitation of a minor; and (C) the defendant did not intend to traffic in, or distribute, such material, *decrease by 2 levels*.

USSG § 2G2.4(a), (b) (Nov. 1, 2006).

Therefore, a defendant who “transported” child porn by taking a laptop with him on an interstate or foreign commerce trip – but didn’t access the porn during the trip – has an argument for this two-level reduction. At offense level I, this is at least an eight month difference in the low-end sentence, if not more.

### C. File Time Stamps: Creation Dates, Modified Dates, and Defenses

The timing of the creation, acquisition, or access to a file can make a significant difference in a child porn case. For example, if one can prove that a traveler who had child porn did not access it while *traveling*, there is a very strong argument for a two-level reduction in the offense level. *See* USSG § 2G2.4(b).

There are two principles that bear emphasis when dealing with time issues and computer forensics. First, the time data associated with a file is almost always generated by the computer on which the file was created or accessed. That means that if the computer was in a different time zone, or it hadn’t been reset for Daylight Savings Time, or its clock was just incorrect, the time data associated with a file created upon it is not reliable.

This is a very frequent problem and it makes time data on computer files notoriously unreliable. For example, one study looked at over three hundred computers on a university network. The computers’ clocks were terrifically inaccurate: four computer clocks were more than *six years slow!* Eoghan Casey, *Error, Uncertainty, and Loss in Digital Evidence*, INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE, Summer 2002 Vol. 1 Issue 2.

A second important principle is that the terms associated with time and computer files are confusing and counter-intuitive. In the forensic world, the term “**file created**” means the time that a file was created *at that location*. If this outline was copied onto a floppy disk, the “file created” date for the file on the floppy would be the date it was copied onto the disk.

This stands in contrast to the terms “**last written**” or “**last accessed**.” Both of those terms refer to actions taken to the file itself. For example, “last written” displays the last date and time that a file was actually opened, edited, and then saved. Hence, the “last written” date for this outline was the last time that I opened it, worked on it, and saved it.

Think about these terms, and you’ll see that they produce the quirk that a “file created date” can be *later* than the “last written” date. Consider this outline. If I last worked on it, and saved it, on my office PC on May 4, 2007 the “**last written date**” will thus be May 4.

Assume, though, that on May 16th I copied the outline onto a thumb drive to take it with me for a lecture. The “**file created**” date for the outline *on that thumb drive* will be May 16, 2007.

Thus, the “file created” date will be almost two weeks *after* the “last written” date.

Bear these terminology quirks in mind when meeting with a forensic examiner, or reviewing electronic evidence produced by the government.

V. **Production of Child Pornography:** Production cases carry incredibly high mandatory minimum guidelines – as shown below, the “basic” production offense carries a *fifteen year* mandatory minimum. Note that this statute – part of the “Child Protection Act”<sup>9</sup> – defines a minor to be younger than **eighteen years old**. It is not a defense to these federal charges that a state jurisdiction has a *younger* definition of minor. *See United States v. Ortiz-Graulau*, 397 F. Supp. 2d 345 (D. Puerto Rico 2005), *see also United States v. Freeman*, 808 F.2d 1290 (8th Cir. 1987).

A. **Child Porn Production Statute - 18 USC § 2251**

1. (a) Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed. 18 USC § 2251(a) [*ed. note: this is the “core” child production statute, though the statute has other subdivisions as well*]
  - a. (e) Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title and imprisoned **not less than 15 years nor more than 30 years**, but if such person has one prior [enumerated sex offense convictions] such person shall be fined under this title and imprisoned for not less than 25 years nor more than 50 years, but if such person has 2 or more prior [enumerated sex offense convictions] such person shall be fined under this title and imprisoned not less than 35 years nor more than life. 18 USC § 2251(e) (emphasis added).

B. **Beware of Cross-References:** Note that the guideline for straight possession of child pornography has a cross-reference. USSG § 2G2.2(c)(1) (Nov. 1, 2006). Under this cross-reference, a defendant can get hit with the very high guidelines for production, *even if the government lacks jurisdiction to prosecute the “production” crimes*. *See United*

---

<sup>9</sup> The Child Protection Act of 1984, 18 USC § 2251 *et seq.*

*States v. Sheepman*, 431 F.3d 1226, 1232 (9th Cir. 2005) (“A district court may base a § 2G2.2(c)(1) cross-reference on the basis of conduct over which the federal government would lack jurisdiction to prosecute.”) In other words, it is small solace that images produced by the defendant fall outside of the statute of limitations, or took place abroad – with this cross-reference, the client still has full exposure for production crimes. *Sheepman* – and the dangers of cross-references – illustrate why “locked” Federal Rule of Criminal Procedure 11(c)(1)(C) deals are so crucial in child pornography cases.

### C. Large Files are Red Flags for Production of Child Porn

Very large image files – and specifically, digital photographs – are often red flags for the production of child porn. Large files are a good place to start in the forensic analysis, and a very good reason to quickly accept a deal to “lower” charges (such as possession or receipt).

Most digital child pornography images are relatively low-quality, “thumbnail” images saved in a small size and small file format. This is because these small, low-quality files load quickly on web pages and transfer quickly over file-servers, Usenet, or e-mail (*e.g.*, via the internet).

The two pictures below illustrate these points. The picture on the left is represents a picture downloaded from a web page. On a web page, this digital image would probably be a “.gif” thumbnail picture. Its size would be 300 by 300 pixels, and the file size may be **3.95 KB**.<sup>10</sup> (Don’t worry about what “KB” means – it’s important only for comparison purposes).

Contrast this with the *original* picture of these San Francisco tourists on the right, taken with



**GIF image, 3.95 KB, 300 x 300 pixels**

a low-end, point-and-shoot digital camera with normal quality settings. That original file was 640 x 480 pixels, and **91.0 KB**.



**JPG image, 91 KB, 640 x 480 pixels**

---

<sup>10</sup> Imagine one “bit” on a computer as being worth a penny. If a “Bit” is a penny, a Megabyte is worth: \$26,221. A floppy disk is worth \$37,758. A CD disk is worth over \$17 million. A 120 gig hard drive is worth over \$33 trillion. A two-page Wordperfect memo is \$450. The average .jpg image file is worth \$12,326. A short .avi is worth over \$ 3 million.

You don't have to understand KB and pixels to understand that **an original picture from a digital camera is vastly larger than files routinely distributed or displayed on the internet.**

Use this fact to direct your forensic examiner. Ask your expert to "float" the largest size image files to the top of the forensic report. If there are very, very large images it is likely that they were downloaded directly from a digital camera. Needless to say, child pornography that appears to have been taken on a client's own digital camera presents a very different sentencing and exposure problem than child pornography saved in thumbnails and traded across the internet. *Compare* USSG § 2G2.1, Exploiting Minor by Production of Sexually Explicit Materials, Base Offense Level 32, *with* USSG § 2G2.2, Possession of Child Pornography, Base Offense Level 18 (Nov. 1, 2006).

The same principle holds true for video files. Under the Federal Sentencing Guidelines, a single video file with child pornography counts for **75 images**, and videos longer than five minutes can merit an upward departure. *See* USSG § 2G2.2 comment. n. 4(B)(ii) (Nov. 1, 2006). Thus, with just eight child-porn videos a defendant can earn a **five offense-level bump** for possessing over 600 "images." USSG § 2G2.2(b)(7).

Video files are huge. An eleven-second, low-quality .avi video clip can be 21.4 MB (22,454,668 bytes). By contrast, the original high-quality photo described above is 93,206 bytes. In other words, a pretty big, good quality picture file is .4% as large as a very short, so-so quality video clip.

Ask your forensic expert to give a list of all big files, and you'll catch original images and video files that are mislabeled, misidentified or partially deleted. Identifying original digital image files and video clips early in the case (before the government does) can dramatically change how attractive an offer looks in a child porn case.

## VI. Miscellaneous Forensic Pointers

### A. Larger Internal and External Hard Drives Increase Dangers in Sex Crime Cases

A big computer hard drive is a bad fact in a criminal case. The bigger the drive the worse the fact.

Of course, the obvious concern is that a bigger hard drive can hold more bad evidence, be it e-mails soliciting fraud, child pornography, or cooked books. That truism, however, doesn't capture the real danger of very large hard drives:

**Large hard drives are dangerous because "deleted" material is more likely to survive,**



**for longer, and is more likely to be recovered through forensic analysis.**

Here is the technical explanation for how file deletion works on a computer:

Your first thought may be that when you ‘delete’ the file, the data is gone. Not quite, when you delete a file, the operating system does not really remove the file from the disk; it only removes the reference of the file from the file system table. The file remains on the disk until another file is created over it, and even after that, it might be possible to recover data by studying the magnetic fields on the disk platter surface.

<http://www.heidi.ie/eraser/> (visited Apr. 30, 2007).

Here’s the explanation in plain English, with some gross generalizations that will drive computer experts nuts. Information on a hard drive is stored with a series of electronic “switches” flipped “on” or “off” – turned to “0” or “1”. That information can physically be scattered all over a hard drive. A computer operating system (like XP or Vista) remembers where these switches are physically located on the disk, and (very quickly) gathers the data up into a file – like a picture, or text file – when the user pulls up the file.

When a file is “deleted” the operating software doesn’t go back and turn off all of those electronic switches on the hard drive. Instead, the operating system makes a mental note that there’s some open real estate on the hard drive that can be *written over* if, and when, new data comes along. The data itself – the electronic “0s” and “1s” – reside safely on the hard drive until overwritten (even if the user believes that the date is “deleted.”)

This no-man’s land of data that can be overwritten is called “unallocated file space” – there is also a related concept called, “file slack.”<sup>11</sup> Unless the client is a very savvy computer person,

---

<sup>11</sup> File Slack Defined:

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called “file slack”. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean more file slack and also the waste of storage space when Windows 95 systems are involved. However, this computer security weakness creates benefits for the computer forensics investigator because file slack is a significant source of evidence and leads.

File slack potentially contains randomly selected bytes of data from computer memory. This happens because DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, DOS/Windows makes up the difference by padding the remaining

when he or she reassures you that they “deleted” incriminating files, this is what actually happened to the data: the incriminating files still may exist, waiting to be overwritten while in “unallocated file space.”

This problem of lingering “deleted” evidence is aggravated by big hard drives in two ways. First, the bigger the drive, the less likely that “deleted” data will be quickly overwritten by new information.<sup>12</sup> Second, the bigger the drive, the sloppier the housekeeping. Users who aren’t worried about hard drives filling-up and computers slowing down (because their hard drives are enormous) don’t take the time to delete old files (*a.k.a.* “evidence.”)

To recap, here are three principles related to deleted files and large hard drives:

1. A file isn’t “deleted” until it is *actually overwritten with other data* (and sometimes the file can still be recovered with forensic analysis).
2. As hard drives become bigger, it is statistically less likely that data “deleted” in unallocated file space will be overwritten with new data.
3. Hard drives lead to sloppy housekeeping. Big hard drives are less likely to slow down from disk clutter, so users are less likely to routinely delete data (“evidence”).

Finally, a corollary of these principles is that storage media that isn’t used by the computer’s operating system (like external hard drives, CDs, DVDs, and the increasingly rare floppy disks) are very dangerous. Indeed, for non-rewritable disks (the vast majority of CDs and DVDs now on the market), the hope of overwritten data can’t come into play.

## B. Tales from the Crypt

---

space with data from the memory buffers of the operating system. This randomly selected data from memory is called RAM Slack because it comes from the memory of the computer. RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

<http://www.forensics-intl.com/def6.html> (visited Apr. 30, 2007)

<sup>12</sup> This assertion isn’t quite as simple as it sounds. Apparently, the newer Microsoft operating systems will always begin by overwriting data closer to the center of the disc “platter.” Thus, even if there is a larger hard drive, with a recent-vintage operating system “deleted” data will be overwritten at a similar rate to an older smaller drive, because the computer tries to keep the (faster) center part of the disk in use.

Nonetheless, as a general matter larger drives will retain “deleted” information longer than smaller hard drives.



Encryption software is becoming increasingly popular, and presents some interesting forensic issues.

One of the most common encryption programs is “BestCrypt.” Here is a description of the software from Jetico’s (the manufacture’s) website:

BestCrypt creates and supports encrypted virtual disks and these disks are visible as regular disks with correspondent drive letters (for example, D:, K:, Z:, i.e. with any drive letter that is not used by other system devices).

The data stored on a BestCrypt disk is stored in the container file. A container is a file, so it is possible to backup a container, move or copy it to other disk (CD-ROM or network, for instance) and continue to access your encrypted data using BestCrypt.

Any free drive letter in the system may be used to mount and to open an encrypted file-container for access. When the virtual disk is opened, you can read and write data as if it were a conventional removable disk.

<http://www.jetico.com/index.htm#/products.htm>

Any forensic examiner will be able to instantly identify encrypted data on EnCase or Forensic Tool Kit: the data looks like a huge lump of a file that doesn’t open easily. The question is, can government examiners open encrypted files on your client’s computer?

Maybe. A forensic examiner can do a forensic search for password strings in EnCase. There is often a record of that data saved on the computer. That process is slow and laborious, but may allow entry into encrypted files.

Another approach is called a “brute force” attack.<sup>13</sup> In a brute force attack, forensic

---

<sup>13</sup> From Jetico’s website: “ I came over website of a company that claims that they can Brute-Force/Dictionary attack BC Container passwords. Is this really true? If it is, why? There should be protection against these things.

Yes, we are aware of companies that provide such service. These programs (password-guessing modules) use Dictionary, or Brute-Force (or some combined ) attack on BestCrypt or any other password-based software.

If someone uses a regular word, phrase, name or something else that can be in the dictionary, a guessing module will define the password quickly. All the years we work on BestCrypt, we strongly recommend people to use passwords strings as random as possible. As some theoretical papers say, a 20-letter English phrase, instead of having  $20 \times 8 = 160$  bits of randomness, has only about  $20 \times 2 = 40$  bits (8 bytes) of randomness. For example, the word “jtBL1@cphER!\*{>” is not an English word or phrase and its randomness is much higher than in the passphrase “In God We Trust”.

examiners run password-generation programs that throw random password combinations at the encrypted file with millions of combinations in an hour. They'll run these programs twenty-four hours a day, for days. See <http://www.lostpassword.com/bestcrypt.htm> (describing software program to recover password keys for BestCrypt).

Sometimes a forensic examiner will get lucky, and the password-guess will work. From a defense perspective, knowing how strong (*i.e.*, how random) the client's password is will help estimate the likelihood that the government's "brute-force" attack will work.

### C. Search Issues (Spam, Spam, Spam)

The hot new search issue in the field of computer forensics is probable cause for computer search warrants. Specifically, can e-mails recovered from *other* computers establish probable cause to search a home user's machine?

That was the issue in *United States v. Kelley*, 482 F.3d 1047 (9th Cir. 2007). In *Kelley*, the defendant's AOL account was searched, then his home computer. The second (computer) search warrant was the subject of this appeal by the government.



Police had investigated a child porn distributor in Germany. Four e-mails on this German's computer were addressed to an e-mail address associated with the defendant, Kelley. These German e-mails had attachments with child pornography. Another investigation in Kansas revealed five e-mails to another Kelley e-mail address, with child porn attachments. District Judge Phyllis Hamilton suppressed the evidence, observing that the search affidavit didn't explain how the Kelley e-mails ended up on the computers of the two traffickers.

The Ninth described the issue in the case as follows: "Kelley and the government agree that unwitting receipt of e-mail containing contraband will not support probable cause . . . The dispute centers on whether the [search warrant] affidavit is sufficient even though it lacks direct evidence that Kelley actually solicited the offending attachments." *Id.* at 1051.

In a disappointing decision, the Ninth Circuit held that "Since the district court's decision in this case, this court has made clear that probable cause to search a computer for evidence of child

---

If your password consists of random characters, the length about 30 characters would be so secure that even far future computational power won't allow intruders to define your password. In practical life random 12 - 15-chars passwords are very strong."

[http://www.jetico.com/index.htm#/bestcrypt\\_faq.htm](http://www.jetico.com/index.htm#/bestcrypt_faq.htm)."

pornography turns on the totality of the circumstances, including reasonable inferences. *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc). In this case, there is a reasonable inference from facts set out in the affidavit that Kelley was not an accidental recipient of emails with attachments containing illicit child pornography. As we conclude that it was fairly probable that child pornography Kelley willingly received would be found on his computer, we reverse.” *Id.* at 1049.

Judge Thomas’s persuasive dissent in *Kelley* explains how the majority abandons Ninth Circuit precedent, and dramatically lowers the showing required for a search warrant. He complains, “We have never held – until today – that mere receipt of unsolicited pornographic material, without more, establishes probable cause to search a residence for child pornography.” He closes by warning of the impact of *Kelley*: “I can well understand the government’s motivation. Child pornography is a scourge on our nation. But every hour, millions of unsolicited and deceptively disguised emails are sent to innocent computer users. Lowering our standards of probable cause to permit government intrusion into private residences based solely on proof of mere transmittal of unsolicited email constitutes an unwarranted erosion of the Fourth Amendment.” *Id.* at 1058.

The only bright spot in the *Kelley* decision is Judge Thomas’ description of the origin of the term, “spam.” (It came from a Monty Python skit: see picture above).

The *Kelley* decision is worth a careful read, because it lays-out what will be the hot new issue for Fourth Amendment litigation: the significance of forensic digital evidence in probable cause showings for a search warrant.

#### D. OMG, ICQ! (LOL)

In the business context, most computer users rely on software-based e-mail that stores



messages in a database on a local hard drive or server (like Lotus cc:\mail or Outlook).

Most clients, however, (and particularly most indigent clients) use free web-based e-mail and instant messaging, like the ubiquitous ICQ, or Hotmail. The good news is that this leaves less of an evidentiary trail than software-based e-mail. The bad news is that forensic analysis still catches plenty of evidence, even from web-based chat and e-mail.

First, many imprudent clients will turn on a feature that will log and capture web-based e-mail and chat. Forensic software is specifically designed to locate and untangle these logs. Thus, a very early question to a client with computer evidence in his or her case is, “were the web e-mail or ICQ chat logs enabled?”

Even for the rare, discrete client who does not enable this logging feature, web e-mails and chats often survive. Many clients who haunt the chat rooms with minors, for example, copy and paste logs of their chats into word-processing software then save that to their hard drive.

Finally, EnCase data also has a disturbing knack for recovering e-mail or chat data from web sessions, even when that hasn't been saved. At times, that data is saved as part of log files buried deep in the operating system's innards. Therefore, if there is web-based chat or e-mails that are going to be a problem, best to push your client for that information early in the case before full forensic review is complete.

### **E. Gadgets will Get You (Cell Phones, Palms, Treos, Blackberries)**

The forensic analysis of gadgets, like cell phones, Palms, Treos, and Blackberries, is less sophisticated and evolved than forensic analysis of computers. There's two reasons for this: gadgets are newer, so the technology hasn't caught up. Equally important, there are so many diverse gadgets, with so many different operating systems and platforms, that there isn't one software program that can easily handle all of them.<sup>14</sup>

For example, for computer forensic analysis of cell phones many examiners routinely use cheap, widely available software that is actually designed for cell-phone owners to back up data. One example is "Data Pilot," software that yuppies buy to back up contacts from their cell phones. <http://www.datapilot.com/>

Gadget evidence is interesting, because while is often very damning, it also less-reliable and clear than computer forensic evidence. One government examiner began his forensic report of cell phones with this disclaimer: "Generally, it is not possible to 'protect' the integrity of data on a cell phone; however, I take steps to insure that any alteration of data is minimized. For example, when I turn the phone on I use a 'faraday'<sup>15</sup> bag to prevent the phone from accessing a local network. I then connect the phone to a computer and use software tools such as PDA Seizure and "Data Pilot" to examine the Phone Book, Received Calls, etc." (emphasis added). One will never see that type of caveat in an EnCase or Forensic Took Kit forensic report.

Because forensic analysis in "gadget" cases is less-evolved than in computer cases, if evidence from cell phones, PDA's, Blackberries, etc. is critical to your case, it is worth considering a direct forensic attack on the accuracy of the forensic analysis and data.

---

<sup>14</sup> For an interesting paper on forensic software tools for cell phones SIM cards, see Wayne Jansen, *Forensic Software Tools for Cell Phone Subscriber Identity Modules*, at <http://csrc.nist.gov/mobile-forensics/publication/pp-SIM%20tools-final.pdf>

<sup>15</sup> See <http://www.forensicts.co.uk/fts-packaging.asp> ("Faraday Bags Radio Protection for your Exhibits: For urgent cases to avoid a phone potentially becoming pin-locked, we offer a radio screened foil bag to protect active exhibits from the ingress of new data such as phone calls or text messages. The exhibit is protected whilst in transit between scene of crime and our laboratories where localised blockers protect the exhibit during examination.")

## F. Cheapskate Forensic Review

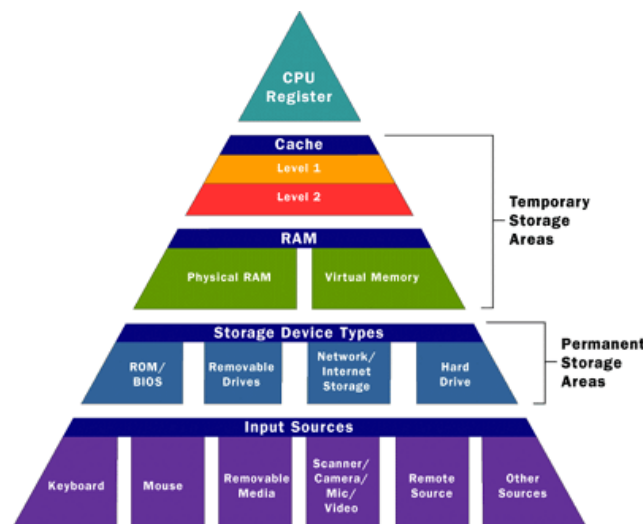
When CJA resources are tight, what is the best bang for the buck in forensic review in federal sex crime cases? Here are some pointers:

- In child porn cases, evaluate the offer by looking for images that create higher guidelines. Videos are prime targets: remember that one video equals seventy images, and six hundred images equals a five offense-level bump.

- Ask a forensic examiner to export web-mail and web-chat logs into .txt files and give them to you for your own review. Buy SuperNotePad for \$30, which will open huge .txt files that would choke Wordperfect or Word. See <http://www.softempire.com/super-notepad.html>. Searching and reviewing these text files yourself helps to cut down on expensive expert time.

- Ask the client. Some cases require a – cautious – approach to the client’s own version of the facts. That isn’t true for sex crime cases involving digital evidence. Push the client for full, open, and early disclosure of everything he or she knows to you. Often, the government has not bothered with a full forensic analysis early in the case, and a client’s insights can help put the value of an early plea offer into perspective. (To be blunt, if the client has been soliciting sex from minors using e-mail, far better that he tell you before the *government’s* forensic expert discovers this evidence on a seized computer).

- A corollary of “Ask the Client” is to get directions from the client. He or she will know where the problem data is stored and can save hours of rummaging through the evidence on forensic software. Even better, ask for a list of questions from the forensic examiner before he or she starts, and get the client’s feedback on these questions to provide the examiner direction during the evidence review. Client-focused forensic review saves time and money.



–oOo–