



# PROTOCOL

A QUARTERLY PUBLICATION

Peace Officer Standards and Training Academy

[HTTP://WWW.STATE.ID.US/DLE/POST/POST.HTM](http://www.state.id.us/dle/post/post.htm)

Michael N. Becar, Director

---

---

## Tracking Internet Crimes Against Children: Tips for Investigators & Other Professionals

*(In March 1998, Supervisory Special Agent Martinez made a presentation on Internet Crimes Against Children at the 14<sup>th</sup> National Symposium on Child Sexual Abuse in Huntsville, Alabama. The following is an excerpt from that presentation.)*

In 1984, the term "cyberspace" was invented by science fiction novelist William Gibson, who envisioned a virtual universe for the interaction of people through computers. Little did he know that such a vision would have serious implications for society a decade later. While the advent of computer and telecommunication technology has allowed children to reach out to new sources of knowledge and cultural experiences, it has also left them vulnerable to exploitation and harm by computer sex offenders. There are no regulatory agencies designated to monitor activities in this "global community," which leaves many of the estimated 10.5 million children who are online vulnerable to adults who may prey upon them.

Reducing the vulnerability of children on the Internet has been the mission of the FBI's Innocent Images Initiative. Innocent Images is the FBI's three-year-old national initiative to identify, arrest and convict individuals who use the Internet and commercial online services to sexually exploit children. This initiative focuses on sexual predators who indicate a willingness to travel for the purpose of engaging in sexual activity with a minor; producers, manufacturers and distributors of child pornography, and collectors of child pornography.

The central operation and case management system for all FBI online child pornography/child sexual exploitation (CP/CSE) investigations is located at the Maryland Metropolitan Office, Baltimore Division. All FBI field offices coordinate their Internet-related CP/CSE investigations with the Innocent Images operation, thereby avoiding duplication of effort.

As part of the Innocent Images National Initiative, the FBI currently has agents online in an undercover capacity in the Baltimore, Houston, Los Angeles, Newark and Tampa offices. It is anticipated that other FBI field offices in strategic locations around the country will eventually conduct online undercover investigations.

The FBI's experience and knowledge base has increased dramatically during the last few years as the result of many changes and the growth of online activity. Following are some of the bits of wisdom and information the FBI has

### LOOK FOR

Using Search Warrants  
in Child Sexual Abuse  
Investigations

2

Upcoming Training and  
New MDT Website


5

---

Continued on page 6

# Using Search Warrants in Child Sexual Abuse Investigations

(The following article is adapted from a presentation Sgt. Fassett gave during the 14<sup>th</sup> National Symposium on Child Sexual Abuse, held March 17-20 1998, in Huntsville, Alabama.)



*PROTOCOL is published quarterly by Peace Officers Standards and Training Academy. This publication is made possible through a grant from the Department of Health and Welfare. The opinions expressed herein are solely those of the author and do not necessarily represent the views of Peace Officers Standards and Training Academy*

*If you would like to contribute an article or have any questions or comments regarding PROTOCOL, please write to P.O. Box 700, Meridian, ID. 83680 Attn. Vicki Yanzuk*

Child sexual abuse investigations are difficult to investigate for three reasons: we usually don't have solid, physical evidence to prove a crime was committed; there are no eyewitness accounts; and it happened to a victim whose credibility may be questioned merely because of his/her age. As a result, it can end up being the victim's word against the suspect's word, and the case may not make it to trial because the prosecutor doesn't have the necessary evidence.

However, police departments have a tool that can reduce or eliminate this swearing match and make the prosecutor's job easier: a search warrant.

Search warrants are used regularly in drug deals, murders, and property crimes, but they are frequently under-used in child abuse investigations, usually because of the belief that they are difficult to write or that only federal officers or prosecutors are allowed to use them. But, in fact, they are easy to write and execute, as long as some basic guidelines are followed.

The role of a search warrant in a child sexual abuse investigation is to add corroboration and credibility to a victim's account of the crime. We don't try to prove a case with a search warrant, but we can force the suspect to do some explaining. The search warrant is an important tool that should be used every time. Combined with the interrogation, it becomes an even more powerful tool that the defense has to work hard to overcome. In addition, it can provide demonstrative evidence, which has a strong effect on juries.

## Practical considerations for the use of search warrants

A search warrant is used to recover physical evidence from a place, person, vehicle, computer, etc. In sexual abuse cases, the most common types of evidence we look for are children's underwear, blood, fibers, hair, and semen. If we don't think we'll find those things, then it may seem as if a search warrant is not necessary. However, this would ignore some of the most obvious and logical pieces of evidence, such as lubricants, sexual devices, and pornography of adults and children. For instance, adult pornography may have been used to lure a teenager in and get him/her to experiment. If we seize the pornography, we can use it to explain to the jury how the offender was lowering the child's inhibitions and we can show them the exact videotape or magazine the victim described.

A case in point is an investigation we conducted concerning the molestation of a three-year old girl by a neighbor in her apartment. Her story was disjointed (which would have made her a poor witness in court), but we were able to understand what happened to her. In particular, she kept talking about playing on the suspect's computer and about a naked version of the Little Mermaid cartoon character. Sure enough, when we searched the suspect's computer, we found the nude mermaid. This doesn't prove the crime happened conclusively, but it added a tremendous amount of credibility to our victim. Realizing that a jury would take notice of this, the suspect pled guilty.

In another case, two young sisters alleged that their grandfather had been sexually abusing them for a long time. The girls said the grandfather would take them to a room without a lock on the door. This made us wonder how he prevented others from walking in on them. Finally, right before the trial was to begin, we questioned the girls again and found out that he would lodge his pocketknife in the doorjamb to keep it shut. When we rushed out to the house, sure enough, we found places all up and down the door where the knife blade had nicked it. So we took a photo of the door and brought it to court. The prosecutor shared it with the defense, and 30 minutes later we had a plea bargain-25 years.

In a third case, a 5-year-old boy had been molested, but we had no way to prove he was in the suspect's house. We asked him to draw a diagram of the interior of the house, and in particular, he remembered an ashtray containing three quarters which was located on a coffee table. The boy had apparently focused on the ashtray while the suspect was molesting him. We went to the house, seized the ashtray with the quarters and then brought in the suspect, who denied that the incident ever happened. It went to trial and the judge sentenced him to 25-30 years because it was obvious that the child had been in the house and the suspect was lying.

A search warrant can also provide information that will assist in the victim interview. I can think of at least five cases in which we conducted a search and discovered that what the victim said wasn't true. It's much better to find that out early than to wait until you get to court. Conversely, sometimes we find evidence that more happened than what the victim says, such as the fact that they may have had full sexual intercourse as opposed to fondling only. One victim insisted repeatedly that she and the offender did not have sexual intercourse, but we found photos proving differently. This prompted us to send the girl for a medical exam, which we wouldn't have done based solely upon her testimony.

#### **A search warrant can identify other victims and offenders**

Child sexual abuse cases are generally not isolated incidents. When offenders are discovered, it's not necessarily because it's their first victim-it's just the first time they've been caught.

Photos, videos, unprocessed film, correspondence and writing can provide clues to other victims or offenders. However, we have to be careful when writing search warrants for these types of evidence because written materials are covered by some constitutional rights. If in doubt, consult with a prosecutor first.

If a person is taking photos of a child and we can articulate that in our search warrant, we ask for undevel-

oped and developed film because we've frequently discovered child pornography or unidentified victims on rolls of undeveloped film.

In addition, it's important to look beyond what the photo initially tells you. For instance, if you have a photo of a victim and the suspect, then you have to find out who took the photo, which means another victim or offender was present.

#### **Executing the search warrant**

When you have your information, move quickly but methodically. Timing is everything. Maximize your element of surprise and the opportunity for non-confrontation. We always try to hit quick, hard and fast and not let them know what we're looking for. We keep it low-key unless the suspect escalates it. We also keep the conversation to a minimum and let him see us moving around, which keeps him worried and helps distract him from making up excuses for why he shouldn't and couldn't have committed this crime.

Always try to obtain the suspect's voluntary consent to the search in case the warrant is later thrown out by the court. However, if you leverage the search warrant, the consent is not voluntary. In other words, don't say, "Mr. Smith, we

want your consent to search your house, but if you don't, we'll search it anyway." The best way to handle it is to knock on the door in a low-key manner and see if he will give consent. If the suspect does consent, we take it and execute the search warrant anyway-every single time. This way, if there's a reversible error in the search warrant and the whole thing is thrown out, we have something to fall back on. We also try to maintain a polite demeanor during the search, because when a person gives consent, he/she has the right to withdraw at any time. When the search is done, we leave a copy of the warrant on the table. But we never say, "By the way, I've got a search warrant, too." We don't bring that into play unless necessary. Just because a judge signed a search warrant doesn't mean it can't be reversed if the court decides you didn't have probable cause. And just because you've never had a previous problem, don't assume you won't have one in the future.

Take all videos listed in a warrant and watch every one of them from beginning to end, even if there are hundreds of them and it takes several weeks. I can't tell you how many times we've found pornography in the middle of unrelated videos. I remember one case in which we found pornography five minutes into a Mickey Mouse Jazzercise tape. The only restriction on taking every video is if the victim said the

**Child sexual abuse cases are generally not isolated incidents. When offenders are discovered, it's not necessarily because it's their first victim-it's just the first time they've been caught.**

**Continued on page 4**

## **Continued from page 3**

pornography was on a specific video, such as one in a black case with red lettering. Then we have to take only that video and we can't touch the others. If you find a tape that looks blank, make sure it hasn't been reversed, which is a common practice in an attempt to avoid detection by the U.S. Postal Service.

Also, take anything that is believed to have been used in the commission of a crime. Then turn it over to the prosecutor and let him/her determine whether it's admissible in court. At the end of the investigation or trial, try to seize all items that are found have been used in the crime. That if the suspect receives probation or is sentenced to only a few years in prison, at least he won't have the equipment and materials to use again.

### **Photograph and videotape the search**

It's important to create a permanent visual record, because the prosecutor and the jury will want to be able to see what you did. Exercise caution, however, when doing it. I personally believe it's a good idea to disconnect the audio portion of the tape because you never know what someone is going to say off handedly that you would not want to have to explain later. Leave the tape silent and then narrate it in court. Also, do not evaluate the evidence on location.

In addition, hold the camera steady. Don't zoom in and out, or you'll just end up making your audience sick. After some embarrassing mistakes, we now send our investigators to school to learn how to operate a video camera. It's also important to have the appropriate equipment if you're going to videotape a search. For example, do not try to use flashlights as a substitute for proper lighting equipment.

At a search scene, everyone has a specific job. We have a scribe, a videographer, a still photographer, and searchers. Everyone stays out of the scene while the videographer records it. When the videographer is done, the still photographer goes in and records it. When the photographer is finished, the searchers go through the rooms and bring items to the scribe, who writes them down, labels them, and lists where they were located and who found them.

### **Writing search warrants**

Search warrants are no more difficult than writing a prosecution report. The two major components are an explanation of your factual belief that the suspect committed the crime and the identification of your source of information.

In chronological order you must be able to explain why you think the evidence still exists at the present location. This is not like narcotics cases, in which you have a very small window of opportunity to look because it can be used up or may not be there. If a suspect has child pornography, he is not going to destroy it get rid of it because he needs it for his sexual fantasies. The only thing

he will do is try to hide it better. Prosecutors might get nervous about this based on the staleness issue, but it really does not apply here.

Search warrants are not based on expertise; they are based on probable cause supported by expertise. I do not like to have my expertise put into a search warrant, because all you have to do is have a few mistakes and then you no longer have your expertise. When we start an investigation, we begin by looking for that one piece of evidence for which we can get a search warrant. When you find it, this will open the door.

Other hints to remember: Don't summarize. Avoid excessive abbreviations. Do not state a conclusion without giving the facts leading to it. Remember that search warrants are subject to open record once they're executed, so be careful what you put in them. The Postal Service offers guides that can help you articulate the wording you need for search warrants.

### **Safety**

Don't assume that child pornographers are not dangerous people. These people will hurt you if given the opportunity. During the last year, eight suspects who were under investigation by our department committed suicide. We have to consider the possibility that they could have just as easily decided that the way to make their cases go away was to get rid of us.

*Reprinted from The National Child Advocate, Published by the National Children's Advocacy Center, Huntsville, Alabama, Vol. 2, No.2 Fall 1998*

# MARK YOUR CALENDARS!!!!

For the 1999 MDT Conference  
sponsored by POST, Dept. of Health and Welfare,  
and Cares



May 6-7, 1999  
Boise, Boise Center on the Grove

Workshops for:  
Law Enforcement  
Prosecutors  
Medical Personnel  
Child Protectors

Focusing on a team approach to child maltreatment.



## NEW MDT Website!!!

sponsored by POST and the Dept. of  
Health and Welfare

For the latest news on MDT happenings in Idaho go to:

[www.idaho-post.org](http://www.idaho-post.org)

Follow the links to other great sites.

## **Continued from page 1**

obtained through tracking and prosecuting individuals who sexually exploit children through the Internet and/or child pornographers who use the Internet:

**1. Offenders believe that commercial services such as America Online are very user-friendly and make it easy for children to use the internet, so that is where they tend to go the most.** Offenders also believe that law enforcement officers are monitoring these user-friendly services, so they are beginning to move to web sites, news groups, and the Internet Relay Chat (IRC), which makes identification more difficult.

**2. IRC channels are basically like the chat rooms on AOL, but the number of channels is almost infinite.** IRC channels are places on the Internet where people can go to communicate with people who have similar interests. To participate, users obtain the IRC software and lists of servers from the Internet and then use their connection to log on, avoiding the commercial online services. The communications are real time, just like telephone calls or face-to-face communications. IRC channels can be dedicated to any topic, including the trading of child pornographic images or the recruitment of children into illicit sexual relationships.

The difference between IRC channels and chat rooms is that subscribers to online service providers that provide chat rooms have unique and traceable screen names assigned to them. IRC channel users can assume any screen name they want and change it at any time. They can assume one identity during one IRC session and another identity during another IRC session just minutes or hours later, which makes identifying and tracking IRC users more difficult, but not impossible.

**3. Pedophiles are also using FServices (automated file trading software) to expand their child pornography collections.** FServices are a feature of IRC channels. An IRC user can set up an FService that allows other users to access and download files from particular dictionaries on his hard disk.

FServices enable computer users to program their computers so that visitors can download a certain number of bytes of information, such as images, in exchange for uploading a certain number of bytes. In other words, it is an automated, computer-programmed trading system. The person who sets up the FService (the host) can establish the parameters of the trading. He can restrict the visitor to certain directories on his hard disk. He can give the visitor a credit for a certain number of bytes or no credit at all. Once the visitor uploads the minimum number of bytes, he can download a preset number of bytes, selecting from the file names listed on any of the directories made available by the host. Most often, a host programs his computer and leaves it on during his absence. The trading is then done automatically by his computer using the parameters the host previously established. Identifying people who establish FServices is done in the exact same way as identifying other users of IRC channels.

**4. One way the FBI identifies and arrests child pornographers on the Internet is by using undercover agents who pose as minors.** In one case, a complaint was received that an offender was sending sexually explicit communications via America Online. FBI agents introduced a fictitious 13-year-old female to the offender and began to correspond with him using this identity. During the two month period of correspondence, the offender sent numerous sexually explicit messages, including two image files containing photographs of children engaged in sexual activity. Subsequently, the offender arranged a meeting for the purpose of engaging in sexual activity. When he traveled to the designated location and approached the Agent, believing her to be the 13-year-old girl with whom he had corresponded, he was arrested. Further investigation revealed that the offender had communicated with close to 200 females and had traveled to two other states where he had met with minor females.

**5. There are numerous federal statutes to assist us.** Some of these laws include: Title 18, USC, Section 2251--Production of Child Pornography; Title 18, USC, Section 2252(a)(2); and Title 18, USC, Section 2422--Coercion and Enticement of a Minor. Foreign governments frequently contact federal law enforcement agencies for copies of our legislation in hopes of getting such laws passed in their countries.

**6. As computer telecommunications have advanced and improved, the cost for this technology has decreased for the consumer.** Not so long ago, child pornography was limited to photos that came from overseas magazines. This has changed with the introduction of video technology and digital photography. The FBI has seen an increase in the number of recent homemade photographs of children that have been scanned onto the internet. This technology also makes it possible for the offenders to easily accumulate thousands of pornographic images and materials.

For example, in a recent case, two offenders were arrested after molesting a 12-year-old boy. When a federal search warrant was executed at the suspects' residence, investigators found four computer systems, one laptop computer, a network server, four printers, a recordable CD-ROM system, a digital camera and two video camcorders. More than 1,700 computer diskettes and recordable CD-ROMS were also recovered, as well as a number of used computer hard drives, videocassettes, and numerous printed photographs. It was determined that the subjects were videotaping their victims, converting the images to CD-ROMS, and distributing them on the internet.

**7. Educating parents and the public about the possible dangers of the Internet is vital.** Everyone, including public officials, law enforcement, parents, educators, and commerce and industry leaders, must be vigilant in and responsible for teaching our nation's children how to avoid becoming

victims of those who wish to sexually exploit them. For example, an FBI agent recently learned of a teacher who was establishing a web page for her grade school students. The teacher was planning to list the students' names, ages, and other personal information. She changed her plans when she realized this was just the sort of information a computer sex offender would love to have.

**8. Law enforcement agencies should encourage their community members to report instances of child pornography and child sexual exploitation they encounter.**

When law enforcement officers receive complaints concerning child pornography and/or child sexual exploitation over the Internet, the following steps are recommended:

- a) Get as much information as possible from the complainant, including their screen name, Internet address, and the date and time they encountered the CP/CSE.
- b) Ask the complainant where they were when they encountered the CP/CSE. Were they on an online chat room, Internet Relay Chat, or browsing news groups? If they were in a chat room or IRC, what was the name of the room or channel they were in? If they were browsing a news group, what was the name?
- c) Determine who sent the child pornography to the complainant. If it was sent with e-mail, the e-mail will show the identity the sender. If it was a news group posting, the person who posted it will be identified in the heading of the post. If the child pornography was sent directly to the complainant during an IRC session, ask the complainant if they have any logs of their activity that might also show the identity of the sender.
- d) Does the complainant have any hard copies of the material, including e-mail? If so, retain those copies. If possible, copy the material from the complainant's hard disk onto a diskette.
- e) After determining the identity of the subject's Internet Service Provider (ISP), subpoena that ISP for the subject's account information. ISPs generally accept subpoenas from anywhere in the United States by facsimile. Be aware, however, that an ISP in another state may only accept federal subpoenas or subpoenas from its own state.
- f) The following information is typically available via subpoena:
  1. name of the account holder, status of the account (active, canceled by subscriber, terminated by the service provider, etc.);
  2. address of the account holder, telephone

- number(s) of the account holder;
3. date the account was established; account usage history;
4. e-mail address belonging to the account holder;
5. for the online service, the screen name(s) associated with the account; and
6. billing method for the account.

- g) After receiving copies or a diskette of the evidence, make sure that the complainant deletes all child pornography from their computer, including any e-mail which might have child pornography attachments.

Often, the complainant may not have saved the attached e-mail and does not remember the sender's identity. In those instances, there is virtually no means available to investigate the offense.

**9. Investigators should become familiar with the Internet and the federal and state laws concerning CP/CSE.**

The FBI, United States Customs Services, United States Postal Service, and the National Center for Missing and Exploited Children (NCMEC) offer training and assistance to local and state law enforcement officers on the complexities of investigating these types of crimes. For more information on training, contact the NCMEC at 703-516-6140.

**10. Law enforcement agencies must also address this crime in a responsible manner.**

Investigating Internet crimes against children raises significant issues with legal precedent, particularly in the area of entrapment. Each law enforcement agency should follow established policies to ensure the successful prosecution of these offenders.

The success of the Innocent Images Initiative is based upon a teamwork concept and involves local, state and other Federal agencies, such as the United States Customs Service and the United States Postal Inspection Service. In the past year, the Innocent Images Initiative has produced a 57% increase in the number of arrests and a 45% increase in the number of convictions. For further information concerning the FBI's Innocent Images Initiative, contact your local FBI office.

*(SSA Martinez is the former Program Manager of the Innocent images National initiative at FBI Headquarters. He is currently one two supervisors assigned to the Innocent Images operation in the FBI's Baltimore Division.)*

*Reprinted from The National Child Advocate, Published by the National Children's Advocacy Center, Huntsville, Alabama, Vol. 2,*

*No.2*

*Fall 1998*

Peace Officers Standards and Training  
P.O. Box 700  
Meridian, ID 83680-0700

# PROTOCOL

---