Investigating Internet Crimes Against Children

Information from
Unit Commander’s Training
National Center for Missing and Exploited Children
26-28 Sep 1999
Alexandria, Va.

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
davecops.org

The Internet knows no boundaries. It doesn’t care about your jurisdictional area; it goes everywhere. We have 80 million people in this country, and perhaps 200 million people worldwide, on the Internet.

Exposure to inappropriate material. Child pornography trafficking is at an all-time high due to widespread use of this technology. People even try to sell babies on the Internet. Offenders very motivated to pursue their fetish, and computers make it easy to keep information on their victims, make contact, trade pictures. They don’t have to go to neighborhood adult bookstores to watch porn movies; they can check a videotape out and see it at home.

These cases are not about computers, but about the sexual exploitation of children.

61% of all rape victims are under 18 years old. Ages between 7 and 13 represent the peak period of vulnerability. 40% of offenders imprisoned for sex offenses reported that their victims were less than 12 years old.

Children are perfect victims:

- Too trusting
- Often desire attention and affection
- Often desire material things
- Are often curious about sex
- Often defy their parents
- Often not viewed as credible witnesses.

Degree of sexual abuse via the Internet ranges from obscene conversation to indecent exposure, display of pornographic material, to fondling and rape.

Disclosure process – Molested kids don’t pick up the phone and dial 911 to report the crime. Some kids (stranger abduction) may report promptly. Others delay disclosing, or give only partial or progressive disclosures. Some children never tell. Some disclosures happen accidentally. They don’t want people finding out. Parents view the history or read the e-mail, and find out. Some disclosures are initiated by others (e.g., film processing lab). If we alert film labs to watch out for child porn, what about computer repair shops, who are likely to come into contact with child porn?

Children may fear punishment for their own prohibited conduct or participation in sexual behavior. Child may fear being grounded from the computer.
Quality investigative interviews are critical to the investigation. Requires special training in how to properly interview kids. The challenge today is you have to explain in court what you have done. Must be legally defensible.

Child molester types…

**Preferential sex offenders**

- True preference for child sex partners
- Usually will have multiple victims
- Will go to great lengths to seduce a child
- Circle of friends are younger (let kids hang out at their house, teen chat rooms on Internet)
- Very skillful at manipulating children
- Numerous victims in their lifetime
- High rate of recidivism
- Well-proven techniques for obtaining child victims (get jobs with lots of child contact)
- Highly motivated to commit sex crimes
- Sexual fantasies focusing on children
  - Homes decorated (teen mags, video and Sega games) and conducive to kids hanging out to have fun
- Collect, produce and trade child porn and erotica

Computer technology and the Internet may have identified and or produce a new offender, the preferential/situational offender.

**Situational offender**

- Not obsessive, doesn’t target kids. But will take advantage of an opportunity to have sex with kids.
- Offender with no criminal record
- Juvenile offender, collection of porn collections with even younger kids

**Legal definition varies by jurisdiction**

- If “real” child is involved
  - Other jurisdictions and feds say if it even looks like a kid, it is actionable
  - This is either a picture of a crime in progress, or one used to entice children
- Child porn used to show to kids to lower their inhibitions

Why offenders collect child porn – made for the offender’s own purpose…

- Sexual gratification
- Lowering child’s inhibitions
- As a medium of exchange
- Blackmailing the victim
- Rarely used for profit

**Jurisdictional issues are not yet worked out…**

- City?
- County?
- State?
- Feds? FBI, Customs, Postal Service, Secret Service (don’t have training, or standing to charge in many sex assault cases)
Who is in charge if it involves multiple jurisdictions?
Sharing of information and resources – how do we do...

- Trafficking in child pornography
- Traveler cases

Publicity – who decides when you announce to the public?

Complex technical equipment as evidence

- Seizure of computer equipment as evidence
- Transportation and storage of computer and related media as evidence
- Forensic evaluation of computer equipment – who has expertise to do analysis?

Complex legal issues

- Know and understand relevant state and federal laws
  - When to use a search warrant
  - When to use court order
  - When to use subpoena

Complex investigative issues

- Identifying the victims
- Interviewing the child about computer-related issues
- Identifying the suspect when kid doesn’t know him face to face
- Interviewing and interrogating the suspect about computer-related issues

Every degree of sexual abuse can be perpetrated by computer – obscene conversation, indecent exposure, display of porn material, fondling, rape.

Computers appeal to offenders

- Tool facilitates their interest in children

- Provides the offender with
  - Privacy
  - Anonymity
  - Instant gratification

- Expands the opportunity for contact with children

1 kilobyte – one typewritten page
1 megabyte – size of average novel
1 gigabyte – 150,000 typewritten pages

Challenges to law enforcement

- Learn and stay current with these technologies
- Overcome the arguments against the need to investigate these cases
- Conduct competent and thorough criminal examinations
- Conduct competent forensic examinations
National Center for Prosecution of Internet Crimes Against Children

Daniel Armagh
darmagh@ncmeg.org
793-837-6337

One of the biggest areas of ignorance among prosecutors and judges in this country is in the area of seizing and searching computers involved in crime. So you NEED a written protocol that has been approved from on high that guides you in doing these things.

Make sure when dealing with the press you have someone who knows the law and doesn’t violate the suspect’s rights (privacy, electronic communications, etc.) as he describes how the computer was taken down.

Court can order your agency to hold an internal investigation into your conduct in seizing and searching someone’s computer.

Don’t make your protocol too specific about what you should be doing.

Policy fundamentals:

• These are sexual abuse cases, not computer crimes cases.
• Computers are not the victims in these cases, they are the tools
• Do not abandon your investigative training when you see a computer

Failure to incorporate the law into your management decisions is asking for disaster.

Privacy issues

• Federal constitutional protections
• State constitutional protections
• Statutory protections
• Court decisions

Federal law apply to ANY computer seizures when attached to the Internet.

Federal privacy statutes:

• Privacy Act
• Stored Wire and Electronic Communication and Transaction Records
• Video Privacy Protection Act
• Protection of Children from Sexual Predators Act (1998)
• Children’s Online Privacy Protection Act

Technology is moving so quickly that the courts are way behind. Calls for monthly shepardizing of the case law.

You must be extremely careful before using a search warrant to obtain evidence from persons who are able to claim that they publish information to the public (i.e., bulletin board sysops) Zurcher v. Sanford Daily Press. 436 U.S. 547 (1978).

Privacy Protection Act 42 USC 2000aa

PPA provides for damages even where officers acted in good faith. PPA applies only to law enforcement.
PPA regulates searches or seizures of work product materials or documentary materials which are intended to be published to the public. (many pedophiles are now putting letters to Bob Guccione in every subdirectory where they have child porn pictures – letter to the editor). Law enforcement may not search or seize work product material from any person who intends to publish information to the public.

Under PPA, almost anyone is allowed to claim they are a publisher. Law enforcement must serve the target with a court order or subpoena which the target may seek to have quashed by a court. The practical effect is to prohibit law enforcement from obtaining records from anyone that claims publisher status.

For a valid claim to be made against you under PPA:

- There must have been a search and seizure, and
- There must be a showing of intent to publicly disseminate the information.

Exceptions to PPA – “any contraband or the fruits of any crime of things otherwise criminally possessed, or which is or has been used as a means of committing a crime. If child porn, you can take down that entire computer system. At some point, the owner could request back the work product materials, and you must give them back, but that person can still be prosecuted.

**You may use a search warrant where:**

- Materials relate to a criminal offense (other than mere possession themselves in hands of innocent third party who intends to publish; though child porn is NEVER protected)
- Immediate seizure of materials is necessary to save lives or prevent serious bodily injury
- In the case of documentary materials only, service of a subpoena would result in destruction, alteration or concealment of evidence, or
- A court order was not complied with, and either appellate remedies are exhausted or delay would threaten the ends of justice.

Documentary materials include any recorded information whether by video, photograph or similar device.

If you take down the computer, and have probable cause to do so, and see protected work product material, you look at everything on hard drive.

Materials associated with bulletin board systems or chat rooms are virtually always covered by the PPA. Arguable in court.

**Special problems under PPA:**

- Poorly drafted language
- Commingled materials – some of the material is protected and some is not; how do you proceed?
- What if you were unaware there is also protected material on the computer until you seize it?
- Copy the disk or the criminal portion of the disk?
- Ensuring accurate copies
- Is law enforcement required to examine every file on the system before removal?
- Letter to the editor in every file of the target’s computer.

Courts are deciding these issues every month, with varying degrees of consistency.

Your job is to draft your affidavit to fit one of those exceptions to the search warrant prohibitions. Case law says that the PPA does not require application for the search warrant to describe exceptions to the PPA.
PPA does not apply to criminal suspects and no greater showing of probable cause for search warrant involving confidential relationships (can bust the lawyer or counselor if they have child porn of their client’s).

Case law on “is this the type of material you can publish” and “is this the type of person who generally publishes this type of material.” “Did he have a reasonable intention to publish this material to the public.”

(See case cites on this law in the Unit Commander training materials binder)

A person can get attorney’s fees and courts costs if they successfully sue a law enforcement officer.

Can go back four years to sue you for violations under the PPA.

Depugh v. Sutton – PPA does NOT protect in cases of child pornography.

VERY supportive case about the hard work police put into these investigations, and giving them the benefit of the doubt: Davis v. Gracey.

Steven Jackson Games – the most important case in this area of the law. Classic case of violating a citizen’s rights under the PPA. Evidence that someone with he BBS service was hacking into government computers. Secret Service seized computers. Court said they didn’t violate the PPA when they seized the computers, but did violate it when Steve Jackson Games asked for the protected material back, and law enforcement did not return it.

Once the material is published, that person can no longer claim protection for stuff on his hard drive under the PPA.

Court has said that sometimes there is no viable alternative to seizing non-evidentiary items and sorting them out later at the office.

Computer at work – If no communication from your employer that you have no expectation of privacy, you may very well have an expectation of privacy. Have employees read this policy and sign and date it if you do have one. Same thing with employee handbooks that say the employer can come look into your computer at any time.

If given a password to a church or library computer, you may very well have an expectation of privacy.

Electronic Communications Privacy Act (ECPA)

Katz v. United States – People talking on the phone have an expectation of privacy. Any attempt to capture conversation is a search. After Katz, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which regulated interception of oral and wire communications.

PPA protects a select group of communicators – media and publishers. ECPA protects communications – electric, wire, magnetic media. Applies to private parties as well as law enforcement. Does provide law enforcement with a good faith defense.

Laws are complex and many issues have not been resolved. Always consult an attorney when faced with these cases.

Communications in transmission that are affected:

- Fax transmission in progress
- Digital pager message not received
• Any data or commands traveling from one computer to another

Law enforcement seldom needs to intercept communications in transmission.

A party to a communication may keystroke monitor a communication in transmission and intercept it. An owner of a computer or pager is a party to the communication.

ECPA mandates use of a search warrant for law enforcement to intercept.

Application for a court order:

• Probable cause specific offense will happen
• Identity of suspect
• Identity of sender of the communication
• Location of target equipment and facilities used
• Period of time intercept is maintained
• Earlier applications? Course of investigation?
• Less intrusive means adequate?

Must meet a higher standard than ordinary search warrant – PROBABLE CAUSE plus showing all less intrusive avenues have been used or considered and were not feasible. State reasons not possible.

Some states have stricter requirements than ECPA.

In monitoring wire transmissions, investigators must stop listening to innocent conversations. Non-relevant material must be deleted before turning this over to someone else involved in the investigation. (Redacted) Failure to redact can cause you lots of legal problems under the ECPA. Keep in main files so you can show that you honestly tried to redact before it went to the investigative file.

You can get stiff penalties for violating the ECPA and even criminal sanctions. But your case will still go to trial. You lose your job, but the evidence is admissible.

E-mail messages in transit are protected until they are downloaded into a computer. Then, you go back to a Fourth Amendment analysis to see if you can access.

Less than 180 days requires a warrant, your choice after 181 days.

No liability incurred by the ISP for disclosing based on the due process instrument you send them.

ISP required under the CPA to notify the customer that records are being requested under a search warrant unless the search warrant specifically says that the officer requests that the customer NOT be notified because of the impending investigation.

Can’t go to video rental place without a warrant to get specific information on customer usage. Wrongful Disclosure of Video Tape Renal or Sale Recods.

Breaking or destroying equipment through negligence is actionable by victims. Loss of business opportunity is actionable by victims, even if criminal activity is part of a wide sweep by law enforcement. Even a perfectly reasonable search which destroys property may be a compensable taking.


Hot topics…
• Interviewing
  • The No. 1 way the defense will try to attack you on how you interview the child.
• Videotaping
  • You better know what you are doing if you use this technique. Suggestive questions?
• Munchhausen Syndrom by Proxy (Factitious disorder)
  • Defense, female perpetrator, escalates abuse of her children in order to get attention. Usually
    escalates to a homicide if you don’t interrupt.
• Plethysmograph
  • Defense, penile polygraph defense, hook defendant up to an electronic device, show different
    pictures, measures blood flow through penis and erection. Defense is I didn’t do it because I can’t
    get it up. Not the issue, but “penetration, however slight.” Effective for therapy, but inadmissible
    in a criminal trial.
• Recantation
  • Investigate why the child took his testimony back. Pressure by someone else who doesn’t want
    this to progress. Do a thorough job of investigation to prevent this.
• Media backlash
  • If you want to be a media star...
• Computer assisted exploitation

Impression Management

• Sound-bite society
• Attention span of jurors
• Educational level of jurors
• Jurors – “not enough evidence” – you are not managing the impression in the courtroom the way we
  wanted.
• Unprofessional mistakes -- -- cop cleaned his nails in court, witness dressed like a slut, hallway
  conversations they thought were inappropriate

Psychology of the Investigator

• Best of the best
• Think like a defense lawyer
• Think like a predator
• Take the testimonial view of everything you do.
• Know your case
• Be organized and concise

Vertical prosecution

• Number of interviews (same people, few interviews so they don’t seem to be inconsistent)
• Target for reasonable doubt
• Coordinated approach
• Prevent meeting new professional every time
• Multi-disciplinary teams

Investigation

• Interview or interrogation is critical to the case
• Safe environment/b his pal
• Lock him into the first five stories
• Miranda
• Consent and warrant
  • Purpose of searching is to corroborate the statements of the child
Corroboration

- Sting
- Non-confession evidence – access, opportunity to be alone, on a green couch, beer in fridge and condoms in drawer.
- Confession – Don’t stop the investigation once you get one. You must prove all the elements of the crime absent the confession.
- Corpus delecti
- Call his mom – have LE interview about character and dynamics of the family. Will help know what the defense will be.
- Interview others
- Anticipate the defense

Substance of Testimony

- Competency
- Remember
- Relate
- Communicate
- Truth and lie
- Punishment

Defense Experts

- What is their previous testimony
- What is their expert background
- Educational relevance – critical to whether they will make a dent in your case

If you do a good job of the forensic processing 90% of these guys will plea.

Offensive Discovery

- Blood typing
- DNA
- HLA
- HIV testing
- STD – sexually transmitted disease – treated?
- Photo corroboration – don’t photograph body parts of perpetrators based on what the kids have old us.
- Forensic computer analysis

Entrapment

The No. 1 defense – the government made me do it.

- Jacobson v. United States
- 112 S. Ct. 1535
- Child pornography
- Reverse sting
- Several agencies over many years
- Political speech issue – 1st Amendment

Other subsequent cases deal with “predisposition” – see case law in training manual.
U.S. v. Gamache

- 1981
- Can apply to chat room and undercover sting protocols
- Non-computer case (mail)
- Travel interstate to engage in an illegal sexual act with minors
- Engage in sex to produce visual depiction
- Defendant must show inducement and lack of predisposition, then government must prove defendant predisposition to engage in criminal conduct beyond a reasonable doubt.
- Improper inducement, time and motive of defendant

Factors Considered in Assessment of Predisposition

- Character or reputation of defendant
- Initial suggestion of criminal activity by government or defendant?
- Def. Engaged in activity for profit?
- Def. Reluctant to engage in conduct by persuaded by government agent?
- Nature of inducement or persuasion by government
- Focus must be defendant before contact with government began

Gamache ruling – Court raised a reasonable doubt that the government improperly induced a citizen to commit a crime that he was not predisposed to commit, thereby requiring a new trial.

Heavy, heavy fine ($50K) if ISPs fail to report child pornography.

Fantasy talk

- Never any intent to act on the communications
- Didn’t really think my e-mail partner was a minor
- I thought this was still America
- I was just going along with the tone set by the other party and laughing about it

Countering Fantasy Defense

- Document actions defendant took in support of his conversation
- Corroborate by overt acts
- Always communicate the “age of the child” in the sting operation, several times if possible

Evidence of intent

- Pornography, erotica, cameras, equipment
- Intelligence that corroborates conversation
- Address books and journals
- E-mail printouts/photos/diaries
- Enticement objects
- Hotel room reservations, contents in the defendants vehicles upon arrival relating to sexual content of conversations
- Messages describe sexual fantasies of target
- Target sends porn to child
- Sends graphic sexual cartoons to child
- Sends morphed sexual pictures to child
- Asks child to send naked pictures
- Sets up face-to-face meeting
Standard Operating Procedures -- Pueblo High-Tech Crimes Unit
Investigative and Technical Protocols -- Internet Crimes Against Children Investigations
3 Oct 1999

- Travels from another state to act on messages about sexual fantasies

No real victim in being

- Luring sting wherein no child in fact was involved
- Factual impossibility is NOT a defense
- Attempts
- Can’t prove age of persons in pictures
- Morphed images – Child Pornography Act of 1996 (Main & California)
- Age of consent under state law is 16
- Case compilation available at NCPCA

Research for an Article

No intent for sexual gratification, merely academic, investigative reporter, just curiosity, preparing the case for law enforcement. Possession is a crime unless you are statutorily exempt. The federal law has not granted any exemptions for child pornography.

Child Pornography

- Unsolicited
- Did not know age of actor
- Was not my computer
- Was not the primary or secondary producer
- Records were stolen or burned
- Home movies – artistic

Computer Pornography

- Determine ownership
- Determine who used computer
- Fingerprints
- Passwords, canceled checks
- Writing exemplars
- Access to common area

SODDI

- My wife
- My roommate
- Someone else loaded it on my computer via the Internet
- Police uploaded porn and put it on my computer
- Did not know child porn on my computer

Other Concerns

- Value added techniques altering electronic evidence
- Mirror image was not done properly, thereby altering the evidence
- Custodian of record-input person not present and therefore suppression is urged
- Police uploaded porn – what belongs to who
- Poor forensic examination

Policies and Protocols
Online protocols which are written guidelines are important
Document your chat logs
Log all undercover activity
Session logs, message logs
Accurate documentation of all undercover activities protects against entrapment defense and provides a stellar record of the best evidence for the prosecutor

Policies on Sting Protocols

- Documentation
- Avoid suggestive screen name
- Use open-ended questions
- You want the target to come off like the pervert, not the undercover officer
- Encourage them to be graphic, just don’t join them

Other Policy Considerations

- Probably a very bad idea to upload porn
- Do not run an investigation from your home
- Early and close contact with prosecutor and investigator is essential
- Use experts – if civilian, always have law enforcement present

Warrantless Searches

- Beware of these
- Withdraw consent
- Never gave consent
- Consent under duress
- Consent plus search warrant – document target’s response

Repairman Case

- Get the call from the repair shop
- Do not instruct repairman to go back and look for more evidence or ever save or download what he saw
- Establish probable cause from description of what he saw before he called law enforcement

Search Warrant

- Demonstrate specific and articulable FACTS showing reasonable grounds to believe that contents of electronic communications or records or other information sought are relevant and material to an ongoing criminal investigation.
- Strong preference for search warrants and courts will scrutinize a warrantless search.
- Most computer searches will be pursuant to a warrant.

Searching Computers

Exceptions apply:
- Plain view, lawful position to observe the evidence and its incriminating character is immediately apparent.
- Determine the role of the computer in the offense
- Repository for storing computer pornography
Exigent Circumstances

- Degree of urgency
- Time for warrant
- Evidence destroyed
- Danger
- Target knows you are coming
- Destructibility of evidence
- Multi-network involved

Border Searches

- Sovereign’s power to exclude
- No warrant required
- No probable cause required
- Once evidence is in country and citizen downloads from BBS, do you need a search warrant to obtain child porn?

Consent Searches

- Spouses: defendant must show spouse actually denied access
- Parents: minor children
- Parents: adult children
- Employees: public/private
- Expectations of privacy
- Objectively reasonable expectations of privacy
- Network systems administrators
- Informants and undercover agents must go no further than permitted by defendant
- Scope exceeds consent
- Proper party consents but data is encrypted
- Limitations on consent either implied or expressed must be honored
- Third party consent to common area

Seizing Hardware

- Contraband
- Instrumentality
- Evidence; physical components – central processing unit, keyboard, monitor, modem and printer
- Peripherals
- Documents /data only

Independent Component Doctrine

- Each component is analyzed independently
- Seize only components that are evidence of a crime
- Officers must articulate a reason for seizing the item
- Not just anything connected

Transporting Hardware

- Handling information storage devices
- Careful packing
Where Might Evidence Be

- Identity investigation
- Fingerprint
- Handwritten notes
- Labels
- Password
- Telephone records
- Hard copy print out

Seizing Information

- Information at the scene
- Information stored off-site
- Contraband – software, access codes, and manuals
- Instrumentality – digital software used in forming collages of children for child pornography
- Information as evidence
- Documents connecting evidence to crime
- Patterns of mailing
- Porn exchange
- History of operating chatroom or BBS – paper or electronic in form

Affirmative Defenses

- Less than three matters of visual depiction
- Promptly and in good faith allow only law enforcement to access visual depiction
- Took reasonable steps to destroy depictions, or
- Reported the matter to law enforcement and allowed access

Orientation to Computer Technology and Online Communications

Marketing technique of porn sites –

In building a web page, they often put in source code behind the scenes a popular phrases hundreds of times so that when a person searches for “Columbine” or some other newsworthy event, the search engines rank that site near the top when someone searches for an innocent-sounding word.

Sexual predators...

- Find victims on the Internet
- Pose as other children
- Find kids in chat rooms, newsgroups
- Transmit and exchange child pornography
- Send unsolicited pornography
- Market kiddy porn

www.terraserver.microsoft.com – Use satellite to zoom into any spot on earth, and see a photo of it.

Coordinating and Conducting the Investigation

Jimmy Doyle, NYPD High Tech Crimes Unit

**Child molesters love the PC**

- Privacy
- Anonymity
- Invisibility
- Instant gratification with tons of pornography, fantasy stories, courting potential victims. Immediate feedback while interacting online.
- Lure children
- Organization – directory structure, boys with boys, girls with animals

Keep diaries, chat logs and journals as trophies.

Many of these online criminals have no prior criminal history.

**Types of Cases**

- Distribution/manufacturing of child pornography
- Possession of child porn
- Endangering the welfare of a child
- Obscenity statutes
- Traveler cases
- Harassment
- Terror threats, theft of identity
- Organized conspiracies
- Child sex tourism

**How the Case Begins**

- Visual evidence, photos, pix, movies
- E-mail messages
- Victim-witness disclosure
- Concerned parent or citizen
- Police undercover activity
- Inadvertent discovery
- Law enforcement referral
- Media referral

**Investigating Methods**

- Physical surveillance
- Victim-witness interview
- Pretext phone call (one on your floppy disk; check it out)
- Pen register
- Electronic surveillance
- Undercover approach
- Informant contact
• Sting operation
• Advanced techniques (sniffers, datascopes)

**Keys to Success**

• Preservation of evidence
• Swift action to collect electronic audit trails
• Focus on identifying the actual violator behind the Internet address
• Exploiting corroborative computer evidence
• Support, resources and time

Memorandum of understanding when performing analysis for outside your agency, overtime and equipment procurement.

**Internet Protocols**

Domain name system – distributed database that is used to map Internet names to their corresponding IP addresses, and vice versa.

Domain name format: security.lucent.com = 135.118231.12

People get blocks of these numbers, and this number is assigned to somebody. The network and host owners can be identified by examining these numbers.

IP addresses are often hidden from recipients, who see only an e-mail address with a domain.

Winipcfg, or from DOS prompt, or from Run, gives you your IP address that you have when you are logged into the Internet at that point.

Useful tools:

Netscan Tools
Netlab
VisualRoute -- Go upstream to the next location that might know about complaints on the bad guy site.
Sam Spade
NeoTrace

Run whois – “whois getting my subpoena?”

Dragon Star Index – [http://ipindex.dragonsar.net/index.html](http://ipindex.dragonsar.net/index.html) – breaks IP addresses into blocks that you can look up.

IP Tools: [http://home.ag.org/iptools.htm](http://home.ag.org/iptools.htm)
Internet Service Provider lookup – [www.isps.com](http://www.isps.com)

Ping command – hey, is that machine really out there, or is it a fake IP address? Use when your whois command doesn’t bring anything back. Equivalent of sonar for subs.

Get book “Takedown” by Shimomura who did Kevin Mitnick.

Mail server logs and access logs from ISPs.

Jim Doyle
Jrdoyle@ix.netcom.com
Innocent Images Task Force

30 agents full-time, and franchises around the country.

Federal violations:

- Interstate travel with intent to have sex with a minor (Title 18 USC 2423b)
- Enticement of a minor to engage in an illegal sex act (Title 18 USC 2422)
- Child pornography (Title 18 USC 2252A)
  - Manufacture
  - Distribution
  - Possession

Check postal inspectors in the jurisdiction in which the perpetrator lives. They may have a file on him from mail action.

Customs Cybersmuggling Center

Arenas of operation:

- Border interdiction
- Smuggling investigations
- International mail
- Child sex tourism
- Centralized databases of information – enter all child porn targets
- Foreign/domestic PD liaison and training
- Forensics

Also:

- International drug trafficking
- International money laundering
- Fraud/intellectual property rights
- International cyber terrorism
- Environmental contaminants
- Weapons of mass destruction
- International child pornography

Forensics and Internet training for local officers once Cyber Smuggling Center is completed.

Do all areas of the Internet crime, not just child porn. Provide assistance to Customs agents in the field in Internet and forensics.

Child porn library -- magazines and videos, good selection of originals, if you need a good copy for court. Trying to digitize.

Customs first agency to initiate Internet child porn stings. Mach 1993. European/Denmark bulletin board system.
Customs has summons authority to get subscriber information; quicker than a subpoena.

Netscan Tools [www.nwpsw.com](http://www.nwpsw.com)

Helpful for IP addresses – [www.arin.net](http://www.arin.net)
Many search engines – [www.gohip.com](http://www.gohip.com)

Child Pornography Record Index (CPRI) -- database to check for info and leads and follow-up.

- Names
- Addresses
- e-mail addresses
- web sites
- nicknames
- internet location
- arrest/conviction data

**Obstacles**

- Undercover pedophile organizations
- Awareness of police sting operations, undercover sites, chatting
- Methods to avoid detection – encryption, hiding files, false info
- Improper search and seizure of the computer
- Evaporation of electronic audit trails (ISPs and newsgroups may retain for 60 days, but may overwrite in only 24 hours)
- Police investigator with little or no computer experience (*them vs. us*)
- International laws and customs – porn not illegal in many countries around the world

**OJJDP ICAC Task Force Program**

Michael Medaris

**Chokepoints**

- Forensic capacity
- Prosecutors intimidated because they haven’t had time to research these cases, or are concerned about the technological aspects