KBSolutions
KNOWLEDGE BASED SOLUTIONS
www.kbsolutions.com

KBSolutions Inc.
1407 Balsam Ave.
Boulder, CO 80304-3535
lists@kbsolutions.com

Beyond Prosecution: Improving Computer Management Of Convicted Sex Offenders

by Jim Tanner, Ph.D., GSLC

Traditional methods of computer forensics are well established in both law enforcement and corporate settings. These methods include rigorous protocols for examining computers which require removal of the computer to a forensic lab. These methods provide excellent prosecutorial evidence. They are not as well suited, however, to the day-to-day management of sex offenders in the community. Given recent case law, denying probationers and parolees access to computers and the Internet is no longer justifiable in other than severe circumstances. We must find simple methods to manage sex offender's computers.

Community supervision officers cannot seize offenders' work computers for simple monitoring purposes, nor can they routinely remove computers from offenders' homes. Even if they could remove offenders' computers, local forensic labs cannot handle the volume of current probation and parole caseloads. As our offenders increase their computer sophistication and anti-forensic software becomes progressively more available on the web, traditionally based computer forensics will become easier to defeat.

Full forensic examinations by trained forensic specialists are a valuable and irreplaceable component of our justice system. The services provided by computer forensic investigators will continue to grow in importance as our culture becomes more computerized and cyber crime increases. However, the computer management services required by the vast majority of community based offenders can be met by typical field officers employing simple to use software and following proper procedure.

Focus Of Forensics

Until recently computer forensics on sex offenders' computers was performed by law enforcement. For law enforcement there is essentially one thing that is actionable - child pornography. More specifically, the only artifacts on a drive that can result in criminal charges are images or movies of children engaged in or suggesting sexual activity. The vast amount of legal pornography (images or movies of adults engaging in sexual activity and text stories of sexual activity) is not criminal and has, therefore, not been the focus of law enforcement's searches. Thus, forensics on sex offenders' drives has focused primarily on finding images or movies of child pornography.

About 70% of all sex offenders are placed on probation nation wide. Most have access to the Internet. Once offenders are convicted, our examinations of their computers must change. We must take a much broader approach to what constitutes contraband and what activities are unacceptable while under supervision. This paper outlines the changes that must occur in our approach to examining the computers of convicted sex offenders.

Reasons To Examine Convicted Offenders' Computers

There are three reasons to examine the computer use of convicted sex offenders:

1. We may seek to gather evidence for prosecutorial goals. This approach seeks to recover evidence of new criminal behavior or significant violations of supervision conditions. The goal of the information collection in this circumstance is to provide evidence to revoke the offender from community supervision. Traditional approaches to computer forensics are best in these circumstances as they preserve the chain of evidence, are soundly supported by case law, and provide expert testimony by forensic specialists in court.

   Under these circumstances, probation and parole officers should always attempt to have trained forensic specialists examine the suspect's computer. Supervising officers who unexpectedly find evidence of major technical violations or new crimes while using previewing software should immediately secure the computer (keep everyone, especially the offender, away from the computer), contact their local forensic lab and follow the lab's instructions.

   We strongly recommend readers go to www.fletc.gov/legal/downloads/bestpractices.pdf and download "Best Practices for Seizing Electronic Evidence, Version 2.0". This document provides non-technical individuals with the state-of-the-art information on how to seize a wide variety of electronic evidence items (computers, cell phones, PDAs, etc.).

However, most situations do not result in major violations or new crimes. Technical violations resulting in revocation hearings require a much lower standard of evidence and often result in the offender being returned to community supervision. These lesser circumstances relate to the second and third reasons to manage offenders' computer use.

2. The second reason for managing sex offenders' computers is to provide proper supervision and containment of the offenders. Our goal here is two fold;

   A. Reinforce treatment prohibitions against access to sexual material
   B. Reduce community risk by increasing the offender's perception of containment.

   Offender treatment is enhanced if supervising officers can assist therapists by enforcing restrictions against viewing sexually explicit materials. Given the volume of sexually explicit material on the Internet and its ease of access, computer management is a critical element in treatment. Effective computer monitoring also sharply increases the offender's perception of "being watched". The psychological effect of knowing all computer activity is monitored cannot be understated. Proper computer management is a tangible and daily reminder of the containment in an offender's life. It enhances community safety simply by its presence.

3. The third reason we monitor an offender's computer use is to assist the treatment agency in understanding the offender. Conducting an examination of the offender's computer early in supervision provides the officer and treatment agency with valuable information regarding sexual interest and intensity. If the intake is done early in supervision, the inspection will likely detect information relating to the offender's computer use prior to being placed on probation. The supervising officer should assume the computer will contain sexually explicit material since the offender was recently convicted for a sex offense. The intake should focus on developing an understanding of the themes and patterns of access to sexual content

Early examination of the offender's computer provides treatment agencies with information about sexual interests previously undisclosed by the offender. This information, along with the frequency of the material's use, is invaluable to the treatment process. Further, it can accelerate the treatment process by forcing important disclosures earlier in supervision and treatment. On-going detection of the type and frequency of minor lapse behavior also enhances treatment efficacy and promotes community safety.

Examining Patterns in Sex Offenders' Computer Use

Probation/Parole and treatment agencies should focus on obtaining estimates of **TRAPS** information in all computer forensic reports. Examining the **TRAPS** factors allows professionals to obtain a more accurate assessment of future risk and management needs, which translates into better containment and enhanced public safety.

Use Pattern	What To Look For
Themes	Did the Offender have apparent preferences regarding types of sites visited (e.g. Teen, Oral, Group, 'Reality', Public, Voyeur, etc.)? What proportion of explicit surfing time was spent on each type of site?
Ratio	What was the ratio of explicit surfing to non-explicit surfing (i.e. porn to non-porn)? What was the ratio of explicit surfing to total computer use (i.e. to non-Internet use)?
Amount	What was the total time spent using explicit materials per week/month? What was the total time spent on the computer per week/month?
Pace	How quickly did the offender move from site to site (or image to image within a site)? [e.g. did the offender view10 sites/pictures per hour or 1,000 per hour?]
Sessions	How long, on average, did each explicit session last? How frequent were the sessions (i.e. daily, twice a week, weekends only, etc.)? How deeply into sites did the offender go (e.g. splash page only, or linked deep into site)?

While no single **TRAPS** component is definitive by itself, examining the pattern created by the integration of all five elements gives the supervising officer and treatment agency a model of the offender's use. This information should be considered when establishing containment. Information gathered during the examination should be forwarded to the entire treatment team. Therapists, polygraphers, and supervising officers should be aware of the offender's surfing patterns.

Supervision and treatment agencies should take special notice when the following are found:

1. Nude or sexual pictures of the offender.
2. Nude or sexual pictures of others which were taken by the offender.
3. Images of the victim.
4. "Trophy" materials (e.g. articles about the offender or crime, pictures/stories of similar crimes or victims, etc.)
5. Beastiality images in any significant number.
6. Non-consensual, coercion, or "reality" sites/stories/images.
7. Sexually explicit stories written by the offender (female offenders may be an exception to this rule).
8. Any amount of cataloging of content by the offender.

Examining a sex offender's computer is gaining a window into their mind. It can often accelerate containment and treatment. It allows us to understand interests the offender is often loath to disclose. People tend to look at what they like. Offenders will not view any significant amount of a specific type of web content if it does not interest them. Moreover, offenders look at Internet materials when alone - it is private and personal behavior. They tend to follow their fantasies and interests. Finding numerous artifacts reflecting a theme indicates the offender has an interest in that theme. Often these themes have little to no relation to the presenting charge.

Of equal importance is the strength of conclusions that can be drawn from finding thematic artifacts on a computer. It is extremely difficult for an offender to deny interest in a specific sexual behavior when the examiner finds 5,000 artifacts of it on the offender's computer. There is no ambiguity in the findings, the artifacts exist and are measurable.

Targets Of Computer Examination

There are three primary targets of a computer exam on a convicted sex offender:

1. Internet History Records (URL records).
2. Image and media searches.
3. Text searches.

Internet History Records

The single best source of information for the supervising and treatment agencies is the Internet History Records. When a browser goes to a web page, a record of that event is stored by the browser in the Internet history file. This record reflects the actual text of the URL call which generated the page. These records are robust and persistent. URL records often hold information concerning an offender's computer use that dates back months or years. All of these records have date/time stamps associated with them. Software designed to recover and analyze URL records can provide important information about the offender. A simple sort of URL records gives the examiner a quick but complete picture of all five TRAPS measures.

Perhaps equally important, URL records recovered from free space often retain their CAM dates. This allows examiners to retrieve data long after it has been deleted and still pinpoint the date/time of the activity. This date time can be important in court hearings.

Examination of Internet history records yields more information than any other method of analysis. URL histories should be the **first target** of any examination of a sex offender's computer. Analysis of these records is the most time efficient method for enhancing containment and promoting change.

Image and Media Searches

For the reasons stated earlier, image searches have long been the mainstay of sex offender computer forensics. Image and media searches are the **second target** of a good examination. Beyond images of child pornography (which constitutes a new charge), there are two types of images that should be of interest to the examiner:

1. Legal sexual content - helps us develop the offender's themes of interest
2. Non-sexual content that is significant.

Legal sexual content

Most of the sexual content on the Internet is legal. It depicts adults engaging in a wide variety of sexual activity. This material can assist us in developing the offender's themes of interest. When an examiner finds patterns in images/media, it should be noted and reported. For example:

Do the artifacts reflect an interest in a specific sex act?
Do they reflect a preference in "partners" (e.g. age, gender, hair color, size, etc.).
Do they reflect any other themes (e.g. exhibitionism, BDSM, etc.)?

Non-sexual significant content

Often missed by many examiners are themes in content that is not sexual in nature. Any significant theme should be reported to the treatment team. Even if the examiner cannot determine the relationship of the theme to the offense, it should be reported. Examples of themes that subsequently turned out to be significant when discussed in treatment sessions are:

Children's web sites (e.g. Nickelodian, Sesame Street) .
Travel or Mapping sites.
Farm equipment sites.
Images of women and/or children (non-sexual).
On-line clothing catalogues.
Model train sites.
Personal Ad (dating) sites.
Genealogy research sites.
Health information sites.
Gaming sites.
E-Bay®
NetFlix®

Text Searches

No computer exam is complete without conducting a text search. Offenders quickly learn that law enforcement searches for images. They often switch from image based fantasy to text based fantasy. The imagery generated in a sex offender's mind by text stories should not be underestimated. Text searches are the **third target** of a complete examination of a sex offender's computer.

Not only will a proper text search uncover erotic literature, it will also provide you with hits on the HTML page text and HTML meta-tag information contained in many sexually explicit web sites. Even sites which are displayed in languages other than English will often contain English meta-tag information to attract more search engines.

We strongly recommend searching sex offenders' computers with the terms "pussy" and "cock" at a minimum. Our research indicates these two terms will identify approximately 95% of all sexual content with less than a 1% false hit rate. These terms regularly appear in erotic stories, web page content, and HTML meta-tag data.

Community Supervision And Probability

Probation and Parole is a matter of probability. Any offender living in the community may be able to engage in illicit activities for some period of time before we catch them. Simply put, offenders whose every moment and action should be monitored are probably not appropriate for community supervision. Our goal in community supervision is to develop systems which reduce, but probably don't eliminate, the window of illicit activity before the offender is caught. We also attempt to establish systems which will catch even single events which are serious violations.

However, no approach to computer management is perfect. There is always the possibility an offender can engage in illicit Internet activities for some period of time before we catch them. Computers have a way of making us believe we can catch everything an offender does. This is simply not the case and we will make ourselves crazy if we try.

Computer management is like everything else we do in community supervision. We set reasonable conditions and monitor them routinely and randomly. Can an offender get away with taking one drink and us not catching them? Of course. Can an offender get away with being late on a curfew and we not notice? Of course. Can an offender visit one or two pornographic web sites and we not catch it? Of course. But if they engage in any illicit activity long enough or often enough, we will find evidence of this and take action. Our goal with computer management is to set responsible conditions of probation/parole and to routinely monitor compliance with these conditions.

Conditions Of Supervision

The value of proper supervision conditions cannot be overstated. Supervising agencies should carefully construct conditions of computer use. Agencies want to be in the position of having a technical violation for simple use of encryption, for example. Supervision agents do not want to be in the position of having to crack encryption systems to see if an offender is violating conditions of supervision. As an example, it is difficult to determine if an offender has used a RAM-kernal boot disk to avoid forensic detection. Therefore, supervision agencies need to be in the position of having a technical violation for simple possession of such software. This is similar to prohibiting the possession of weapons or burglary tools. Interestingly enough, some encryption software is considered munitions and it is a Federal Offense to export it outside the United States. If it's a weapon for export, it seems reasonable it could be a weapon for an offender.

Properly constructed conditions should clearly prohibit:

A. Use of the Internet to access sexual content of any nature and in any form
B. Use of web based email programs which provide anonymity.
C. Possession or use of programs or systems which allow the device to be booted into a RAM kernal.
D. Use of encryption and/or password protection of data
E. Destroying or altering computer use records - including deleting Internet History Records and restoring operating systems.
F. Cleaning or wiping hard drives.
G. Use of anti-forensic software or processes.
H. Obtaining or retaining "trophy material".
I. Visiting sites which focus on the culture of potential victims.

A sample computer conditions form may be found at www.kbsolutions.com/socompcnt.pdf .

Need For On-Going Supervision

Recently Dr. Steve Brake (www.stephenbrakeassociates.com) and I constructed guidelines to help Probation/Parole officers determine the need for on-going computer monitoring of convicted sex offenders. Our assessment of the need for on-going computer monitoring is found on the next page.

DETERMINING NEED FOR INTERNET MONITORING:
INTERNET BEHAVIOR AND RISK FOR CONTACT OFFENSES

Need For Computer Monitoring While Under Supervision

Behavior						
	VERY-HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH
	MOD-HIGH	MOD/HIGH	MOD/HIGH	HIGH	HIGH	HIGH
	MODERATE	MODERATE	MODERATE	MOD/HIGH	HIGH	HIGH
	LOW-MOD	LOW/MOD	LOW/MOD	MODERATE	MOD/HIGH	HIGH
	LOW	LOW	LOW	LOW/MOD	MODERATE	MOD/HIGH
		LOW	**LOW/MOD**	**MODERATE**	**MOD/HIGH**	**HIGH**

Actuarial Risk of Contact Offense

Y-Axis – "Behavior"

Historical Internet Styles Related to Child Pornographic Images

LOW: Reactive type of user: Incidental use, downloads small amounts of pornography when prompted, OR, less than 1 hour per month spent viewing pornography.

LOW-MODERATE : Active user of pornography: Actively seeks images via web pages, OR, more than 1 hour per month but less than 10 hours a month spent viewing pornography.

MODERATE: Collector behavior: Actively seeks pornography through file sharing or catalogues material, OR, more than 10 hours a month but less than 30 hours a month viewing pornography.

MODERATE-HIGH: Engager behavior: Solicits or grooms children on-line.

HIGH: Abuser behavior: Engages in sex with child met on-line, OR, more than 30 hours per month viewing pornography.

VERY HIGH: Promoter of commercial behavior: Produces or distributes child pornography.

X-Axis – "Actuarial Risk of Contact Offense"

Risk for Contact Offense Derived from Actuarial Risk Assessment Instruments (e.g. RRASOR, MnSOST-R, STATIC/STABLE/ACUTE)

LOW
LOW/MODERATE
MODERATE
MODERATE/HIGH
HIGH