

Rethinking Computer Management of  
Sex Offenders Under Community Supervision

Jim Tanner, Ph.D., GSLC  
President, KBSolutions Inc.  
www.kbsolutions.com

**An earlier version of this article can be found at [www.kbsolutions.com/rcm-old.pdf](http://www.kbsolutions.com/rcm-old.pdf). This older article also appeared in the Journal of Offender Monitoring, Volume 15, Number 2.**

## The Problem

As the Internet and computers become a larger part of our work and personal life, the appropriate monitoring of a sex offender's computer use becomes more important. In recent years computers and the Internet have become widely used. Internet use currently grows at a rate of two million new users a month in the United States. Recent estimates show about 73% of Americans are now online ([http://www.pewinternet.org/pdfs/PIP\\_Internet\\_Impact.pdf](http://www.pewinternet.org/pdfs/PIP_Internet_Impact.pdf)) Denying probationers and parolees access to computers and the Internet is no longer justifiable in other than the most severe circumstances. Recent case law ([www.kbsolutions.com/CaseLaw.pdf](http://www.kbsolutions.com/CaseLaw.pdf)) reveals the courts agree sex offenders cannot be denied access to the Internet.

Computer and Internet access poses substantial risk to proper treatment and containment of sex offenders. The prevalence of sexual material on the Internet makes it risky for convicted sex offenders to have unmanaged access. Various search engines estimate 60 million pages of sexually related content currently exist on the Internet. Newsgroups available through broadband Internet connection have more than 1,600 forums whose titles indicate sexual content. There are few Internet users who have not received at least some unwanted email containing sexual content.

Not only does the Internet present a repository of sexually related materials for sex offenders, it also presents a pool of potential victims. More than ninety percent of children between the ages of 5 and 17 now use computers. More than sixty-five percent of youth aged 10-17 use the Internet ([www.ntia.doc.gov/ntiahome/dn/index.html](http://www.ntia.doc.gov/ntiahome/dn/index.html)). In a study of youth aged 10 to 17 who use the Internet regularly, 20% indicated in the previous year they had received a sexual solicitation over the Internet while 25% reported an unwanted exposure to pictures of naked people or people engaged in sex ([www.missingkids.com/download/nc62.pdf](http://www.missingkids.com/download/nc62.pdf)).

Roughly eighteen thousand sex offenders are arrested in the United States each year ([www.albany.edu/sourcebook](http://www.albany.edu/sourcebook)). On average, 60% of the sex offenders convicted are placed on probation in the community. In Colorado, sex offenders account for approximately 17% of the prison intakes and 27% of the daily population. This proportion is likely reflected in every jurisdiction in America. As the numbers of sex offenders under supervision swells, managing their use of computers and Internet use becomes more important.

Traditional methods of computer forensics are well established in both law enforcement and corporate settings. These methods include rigorous protocols for examining computers. Generally, a computer is seized to allow the examination. A bit stream image of the drive is taken to preserve evidence. Copying the drive often takes hours on drives as small as 20 gigabytes. Copying the larger drives commonly found in current computers can tie up both the suspect's computer and forensic machines for much longer periods. After a copy of the suspect drive is obtained, the forensic investigator must systematically examine the contents. Using EnCase®, Forensic Toolkit®, or X-Ways Forensics®, it takes experienced investigators many hours to fully examine even a small (20 gigabyte) drive. To do a thorough job, forensic examiners need about two days for each drive image.

Traditional methods of computer forensics provide excellent prosecutorial evidence. They are not as well suited to the current day-to-day computer management needs of sex offenders in the community. We cannot seize offenders' work computers for simple monitoring purposes, nor can we routinely remove computers from offenders' homes for monitoring. Even if we could remove offenders' computers, local forensic labs cannot handle the volume of monitoring tasks presented by the current caseloads of officers supervising sex offenders in the community. Moreover, 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.

## The Solution

This article articulates a modified approach to the management of sex offenders' computer and Internet use. This approach, initially developed for the 20<sup>th</sup> Judicial District in Colorado, has become standard practice in many jurisdictions across the United States (see [www.kbsolutions.com/beyond.pdf](http://www.kbsolutions.com/beyond.pdf) for a brief explanation of the principles involved in this approach). The "Managing Sex Offenders' Computer Use" course is currently taught for the American Probation and Parole Association and the National Law Enforcement and Corrections Technology Center (an outline of the course is found at [www.kbsolutions.com/forensicclass.pdf](http://www.kbsolutions.com/forensicclass.pdf) and excerpted slides from the class are found at the end of this paper). This simple approach has resulted in higher levels of sex offender containment, increased supervising officer satisfaction, and multiple offender revocations for inappropriate computer use. Perhaps equally important, it is low cost and supervising officers can quickly and easily manage offenders' computers without burdening local forensic laboratories.

The effective management of community based sex offenders' computers takes five steps:

- 1) understand the reasons for computer management.
- 2) establish clear conditions that are computer specific.
- 3) conduct an intake early in supervision.
- 4) install monitoring software.
- 5) monitor the computer frequently.

### **First Step:** Understand computer management

There are three reasons to manage the computer use of sex offenders. First, 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.

Supervising officers who believe offenders have committed a new crime should not attempt to search for evidence. Under these circumstances, officers should always have trained forensic specialists examine the suspect's computer. Supervising officers who find evidence of major technical violations or new crimes using the monitoring techniques described in this article should immediately secure the computer, contact their local forensic lab and follow the lab's instructions. Fortunately, most situations do not result in major violations or new crimes. These lesser circumstances relate to the second and third reasons to manage offenders' computer use.

The second reason for managing sex offenders' computers is to provide proper supervision and containment of the offenders. Our goal here is two fold; 1) reinforce treatment prohibitions against access to sexual material, and 2) 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.

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 is able to provide 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. Early detection of repeated or significant lapse behavior promotes timely revocation.

**Second Step:** Establish clear, specific conditions.

The value of proper supervision conditions cannot be overstated. Conditions should be carefully worded to avoid violations of the rights afforded offenders under the Constitution and the Electronic Communications Privacy Act. Conditions should clearly prohibit use of the Internet to access sexual content of any nature and in any form, use of web based email programs which provide anonymity, use of encryption and/or password protection of data, destroying or altering computer use records, cleaning or wiping hard drives, and the use of anti-forensic software. Conditions should also include offender permission for unannounced examination of the system, offender responsibility for all data found on the computer, and offender permission for seizure of the equipment in the event of violation. A model Computer Use Agreement adopted by Colorado Judicial Department is available on the resources page of our website ([www.kbsolutions.com/socompnt.pdf](http://www.kbsolutions.com/socompnt.pdf)).

**Third Step:** Conduct an intake early in supervision.

As indicated above, the purpose of computer management of sex offenders is to prevent or deter future illicit use. Our goals in conducting an intake are three fold: 1) determine the extent and type of sexual interests as indicated by materials present on the hard drive; 2) deletion of inappropriate images and text to help eliminate the offender's "cache" of sexual materials; 3) preparation of the hard drive for future examinations.

When first sentenced to probation, each offender's computer should be examined by the supervising officer. The system should be searched for both images and text that are sexually related. I recommend searching the drive's free space (unallocated clusters) along with the undeleted files on the computer. There are a number of high quality integrated forensic suites available which allow officers to conduct such searches. They vary in power, ease of use, cost, and customer support. Several of the more popular integrated suites are listed below.

#### **Selected Commercial Integrated Examination Packages**

Forensic Tool Kit® published by [www.accessdata.com](http://www.accessdata.com)  
EnCase® published by [www.encase.com](http://www.encase.com)  
X-Ways Forensics® by [www.x-ways.net](http://www.x-ways.net)  
ProDiscover® published by [www.techpathways.com](http://www.techpathways.com)  
Professional P3® published by [www.computercop.com](http://www.computercop.com)  
Omniquad Detective® published by [www.toolsthatwork.com](http://www.toolsthatwork.com)  
MacForensicsLab® published by [www.macforensicslab.com](http://www.macforensicslab.com)

#### **Selected Freeware Field Examination Packages**

Field Search published by [www.justnet.org/fieldsearch](http://www.justnet.org/fieldsearch)  
Helix® published by [www.e-fense.com/helix/](http://www.e-fense.com/helix/)  
SPADA® published by [www.cops.org](http://www.cops.org)

I use Field Search (published by the National Law Enforcement and Corrections Technology Center) as my primary intake tool. I recommend Field Search as the tool departments should use for field exams by officers not trained as forensic specialists. Field Search ([http://www.kbsolutions.com/html/field\\_search.html](http://www.kbsolutions.com/html/field_search.html)) is a quick, easy to use program that allows officers to customize their search to offender type and print reports which contain examples of findings. With minimal training, the officer runs Field Search from a USB drive. It finds every logical picture and video on the computer and displays it for the officer to review. Results of text searches are organized in a simple structure and can be sorted by the words found. URL histories are extracted from caches (and free space if the officer selects). Pictures, URL records, or text segments which are considered noteworthy can be easily tagged and included in an easy-to-build report. The report includes other important information like the full path of the file and CAM dates (Created, Accessed, and Modified) for each item reported. The report can be saved to removable media as either a Rich Text File or an Adobe Acrobat PDF® file.

Unless the images constitute a new crime (child pornography), retrieval of this information should be viewed as part of the intake-assessment. It can be extracted, filed, and forwarded to members of the offender's treatment team to assist in developing a comprehensive containment and treatment plan.

It is important to search for text files containing sexually explicit words. A search for images alone is not sufficient when working with sex offenders. While image searches are almost always productive, I have found text searches provide a significant proportion of the findings on sex offender's computers. Often text searches lead to the documents which provide keys to behaviors the offender has not yet disclosed. As each word in the search increases search time, limit the list to four or five words. Searches for slang terms relating to female and male genitalia are especially productive. There are a number of software packages heavily marketed to supervising agencies which search only for images on a hard drive. I do not recommend these packages be utilized.

Once the findings are extracted, all inappropriate material should be deleted from the hard drive. Deleting the material and then emptying the "Recycle Bin" is insufficient to remove the data from the drive. Wiping or overwriting software should be utilized to completely destroy the files. As preparation of the drive for monitoring, wipe the drive's free space as well as the file slack space. Wiping free and slack space at intake (especially with a designated wipe pattern) enhances the evidentiary strength of subsequent findings.

### **Useful Secure Deletion Software Packages**

Eraser 5.3 published by [www.tolvanen.com](http://www.tolvanen.com) - freeware  
AnalogX Super Shredder published by [www.analogx.com](http://www.analogx.com) - freeware  
CyberScrub® published by [www.cyberscrub.com](http://www.cyberscrub.com)  
BCWipe® by [www.jetico.com](http://www.jetico.com)  
Secure Clean® published by [www.accessdata.com](http://www.accessdata.com)  
WipeInfo® published by [www.symantec.com](http://www.symantec.com)

#### **Forth Step:** Install monitoring software

Once the computer has been cleaned, install monitoring software. Monitoring the computer has several distinct advantages over traditional forensic investigation. First, since it actually captures what the offender is doing, it increases the probability of catching offenders who try to defeat forensic tools by using techniques such as layered images, encryption, steganography, or simply putting images inside other applications (e.g. JPG images buried in Word Documents). Detection of these "masking" practices using standard forensic techniques is time consuming and requires specialized training. A field officer using properly configured monitoring software would catch the offender attempting to use these techniques.

Second, monitoring software can reveal the contents of items viewed or manipulated (but not printed) from removable media. Standard forensic approaches rely on artifacts being found in logs, swap files and print spool files to detect this activity. Sophisticated users can view and manipulate material in ways that leave an extremely limited trail for standard forensics to detect. Properly configured monitoring software will create a clear trail of the offender's actions. In brief, monitoring software will increase the probability of catching certain types of illicit computer activity.

Third, monitoring software is more time efficient. As indicated above, it takes days to get the results from a standard forensic investigation of an offender's computer. Using monitoring software, a supervising officer can review a month of the offender's computer usage in about 10 minutes. More importantly, the officer is the one actually reviewing the computer use, so the information is immediately available.

Monitoring software comes in a variety of packages. Essentially, they all work the same. When the computer boots, the software automatically runs. The software hides in the background and routinely captures the computer's activity for later retrieval. Some programs even automatically forward the usage reports to the officer via email. Most monitoring programs are software selectable to capture pictures of the actual screens on the computer, email exchanges, chat room participation, Internet activity, and every keystroke typed. Usually the monitoring software hides its data on the drive in encrypted files and the software is password protected to prevent offenders from turning off the process or seeing the parameters of monitoring.

## **Popular Monitoring Software**

Spector Professional® published by [www.spectorsoft.com](http://www.spectorsoft.com)  
Spector Professional for Macintosh® published by [www.spectorsoft.com](http://www.spectorsoft.com)  
E-Blaster® published by [www.spectorsoft.com](http://www.spectorsoft.com)  
CSWeb®) published by [www.securitysoft.com](http://www.securitysoft.com)  
ActMon® published by [www.iopus.com](http://www.iopus.com)  
Impulse Control® published by [www.InetPPC.com](http://www.InetPPC.com)  
Cyber Sentinel® by [www.securitysoft.com](http://www.securitysoft.com)  
TrueActive® published by [www.trueactive.com](http://www.trueactive.com)  
Desktop Surveillance® published by [www.toolsthatwork.com](http://www.toolsthatwork.com)

Based on cost, ease of use, functionality, support, and security issues we selected Spector Professional® as the monitoring software used in our jurisdictions. The software installs off a CD or USB drive in about 2 minutes. During installation the officer sets passwords and hot keys to activate the review program. The officer can also select which elements of computer use to track, the frequency of tracking, and the length of time the tracking records are left on the offender's computer. Screen sampling can be set to occur in any range between once a second to once every 10 minutes. Once installed, the program automatically starts each time the computer is turned on.

High risk offenders may need the additional management provided by remote monitoring applications. Remote monitoring mirrors the offender's activity or violations to a secure server. A supervising officer can log into these servers from any computer with Internet access to view the offender's activity. Remote monitoring applications provide the officer with expanded ability to manage a sex offender's computer use.

## **Remote Monitoring Applications**

Impulse Control® published by [www.InetPPC.com](http://www.InetPPC.com)  
CSWeb® published by [www.securitysoft.com](http://www.securitysoft.com)

Most monitoring software records the date and time as well as the program operating when screen captures are made. When offender lapses are detected by review of the monitoring records, the captured screen can be printed or sent to a file on a floppy disk for inclusion in reports, filing of violations, or as support for seizure of the equipment. Exported data includes the program active at the time the screen was viewed and the associated date/time.

Monitoring software can reflect all email, both sent and received, can be captured as can all chat room activity and Peer-to-Peer activity. If desired, most applications allow the the supervising officer to set the software to capture every keystroke typed into the computer.

The offender pays the license fee of the monitoring software installed on his computer. Licensing fees can vary widely. In October of 2007, monitoring software costs were ranged from \$40 a year (CSWeb®) to \$300 a year (Impluse Control®) or had one-time fees of approximately \$100 (Spectorsoft products). See the excerpted slides at the end of this article for a comparison of popular products.

Ensuring the software has no conflicts with existing software is important to avoid computer seizure and/or data loss by the offender. While most monitoring software currently on the market is carefully crafted to avoid conflicts, each product should be tested to ensure a specific computer configuration does not cause problems.

Probation and Parole Departments must take care when installing monitoring software on offender's computers. Carefully worded permission should be obtained in writing to ensure the rights of the offender or others using the computer are not violated. Supervising officers should be familiar with search and seizure laws, the Electronic Communications Privacy Act, and the Patriot Act. An excellent review of the legal issues involved is published by the United States Department of Justice and is available at [www.cybercrime.gov/searchmanual.htm](http://www.cybercrime.gov/searchmanual.htm). Interestingly enough, there may be far less legal exposure when installing properly authorized monitoring software than when attempting routine searches of a computer using forensic software.

Marc Harrold at the National Center for Justice and the Rule of Law has written an excellent article on "Virtual Home Visits" and the 4th Amendment. I recommend reading this article. It can be found on the NCJRL website at ([www.olemiss.edu/depts/law\\_school/ruleoflaw/pdf/05-HARRO.pdf](http://www.olemiss.edu/depts/law_school/ruleoflaw/pdf/05-HARRO.pdf) ).

Permission to install monitoring software should be in writing and include disclosure the software is installed. The offender should affirm an understanding of what the software does and that the records of computer use may be used against them in court. The offender should affirm an understanding of the right to refuse installation, indicate the offender voluntarily agrees to the installation, and specifically state the offender holds the agency harmless for any complications arising out of the installation and use of the monitoring software. A copy of an intake agreement is available on the resources page of [www.kbsolutions.com](http://www.kbsolutions.com).

If the computer is a work computer, written permission from the owner of the computer must be obtained to install monitoring software to avoid violating the Electronic Communications Privacy Act. This permission should include a statement that the owner will inform each user of the computer that his/her computer activity is being monitored. The permission should also include a hold harmless clause for any complications arising out of the installation and use of the monitoring software.

Programs which email results to the supervising officer or allow real-time monitoring ( E-Blaster®, Trueactive®, Impulse Control®, and CSWeb®) are beneficial for officers who must travel great distances to visit the offender. For example, in Colorado some jurisdictions fall on two sides of high mountain passes making travel between opposite ends of the jurisdictions time consuming and sometimes impossible due to weather conditions. Many monitoring packages also allow the officer to set “switches” which cause the software to email the officer when an offender violates a rule. The face value of remote programs and email notification is undeniable. However, the allure of not having to leave one’s office to review computer activity of offenders should be carefully examined. Its unlikely that officers receiving 40 to 50 lengthy emails will read them thoroughly. This makes it easy to inadvertently miss important information which is present in the official file.

Moreover, most jurisdictions require a minimum of monthly home visits for sex offenders to ensure living conditions are appropriate (e.g. no boxes of toys or bags of candy in the apartment of a convicted pedophile, no sexually explicit magazines or movies laying around, etc.). Given that an officer can review a month’s worth of computer activity in 10 minutes or less, examining the computer use when making home visits seems a more reasonable approach. It also allows immediate seizure of the equipment if major violations are detected.

I recommend real-time 24/7 monitoring programs (Impulse Control®, CSWeb®) be used when an offender’s risk warrants. In these extreme cases, I believe officers should focus on removing the offender from the community. Real-time monitoring may be the only prudent way to protect public safety while the officer collects evidence to remove the offender from the community.

**Fifth Step:** Monitor the computer frequently.

Failure to properly review the results of monitoring software sends a message to the sex offender that they are not being watched. Computer use should be reviewed monthly. Bi-monthly is marginally acceptable, but less frequent than that is inappropriate. Remembering that one of the goals of computer management is increasing the offender’s perception of “being watched”, infrequent review of computer use defeats this purpose. As indicated above, it takes only 10 minutes to review a month of heavy computer use. Often officers require offenders with notebook computers to bring their computer with them when reporting to the probation offices. This increases the ease of review.

### **Who Needs Monitoring?**

The decision to monitor sex offenders’ computers should be guided by risk assessment. Dr. Steve Brake and I have developed a grid to assist officers in making this decision. This grid is available on Dr. Brake’s website ([www.stephenbrakeassociates.com](http://www.stephenbrakeassociates.com)) and at [www.kbsolutions.com/monitorgrid.pdf](http://www.kbsolutions.com/monitorgrid.pdf). A synopsis of this grid is found in the excerpted slides at the end of this article. In general, most all convicted sex offenders who show more than a low actuarial risk and low Internet usage should have their computers monitored. Even offenders without access to the Internet can view sexually explicit material on their computer, thus reifying deviant conceptualizations and thwarting treatment goals.



## Conclusion

While this article has focused on sex offenders, the steps and tools recommended here apply equally well to cyber criminals in general. Computer use is rapidly growing in the United States. Many offenders must have access to computers and the Internet to engage in lawful employment. Unless absolutely necessary, banning a cyber criminal or sex offender from computer use and Internet access may also block the individual from responsible employment. We need to develop policies and practices which allow offenders to access computers while providing for public safety.

To this point we have relied on computer forensic specialists to help us monitor cyber criminals and sex offenders. The sheer volume of work most computer forensic labs currently endure no longer allows us this privilege. While standard computer forensics can reveal a great deal about computer use, the amount of time it often takes to extract this information is not realistic for community based supervision. Moreover, seizure of the equipment to allow the investigation is generally not possible. We must develop methods which can be accomplished quickly and by field officers who have little to no training in computer forensics.

This article proposed such practices. Jurisdictions in Colorado have identified tools and developed methods which allow field officers to successfully manage computer use of offenders. Intake practices which take approximately 45 minutes include a brief examination of all images on a computer and selected text searches of the entire drive. Information gained from this intake benefits both the supervising agency and the treatment agency. Monitoring software is installed during the intake.

Each offender's computer is reviewed monthly by field officers during home visits or remotely. This process takes approximately 10-15 minutes. This routine review of computer activity increases the offender's perception of being "watched" which, in turn, increases the containment of the offender.

Current practices among probation and parole agencies which rely on overburdened forensic labs results in offenders computer usage not being monitored. While the sampling of computer activity through monitoring software does not ultimately yield as much information as a full forensic investigation of a seized hard drive, it clearly provides far more information than a computer that remains unexamined. Moreover, monitoring software samples all activity on the computer, including activity which took place primarily (or solely) on removable media which is subsequently not available to the supervising officer or forensic specialists.

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. The proposed method of field monitoring accomplishes these goals with far less demands on the limited resources of computer forensic investigators.

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. This article is not suggesting field officers can duplicate or replace these services. It does submit, however, the computer management services required by the vast majority of community based offenders can be met by typical field officers using the proper software and following proper procedure. An officer who suspects new criminal activity should not inspect the offender's computer, it should be examined by a trained computer forensic specialist.

---

Dr. Tanner is the President of KBSolutions in Boulder, CO. He has 37 years experience in community based corrections and has been supervising sex offenders since 1970. He currently provides forensic analysis services to Colorado's 20<sup>th</sup> Judicial District Probation Department. He developed and teaches classes on Field Forensics for APPA and NLECTC. He has provided training on sex offenders, computers and the Internet to a wide variety of national and international audiences. He may be reached at [lists@kbsolutions.com](mailto:lists@kbsolutions.com).

Slides excerpted from Dr. Tanner's class "Managing Sex Offenders' Computer Use"



## What Is Field Search?

Field Search is a software tool that allows non-technical officers to quickly preview and examine computers in the field.



© Copyright 2007 by Jim Tanner, Ph.D. All rights reserved.

## Where Did Field Search Come From?

### Conceived by Jim Tanner



Dr. Tanner recognized the need for a tool that could be used in the field by non-technical officers. KBSolutions developed the initial specifications for Field Search.

### Developed by Jim Persinger



KBSolutions contracted with a leading forensic examiner/programmer to develop the tool. PM Investigations provided development time at substantially reduced rates.

### Funded and Distributed by NLECTC



Joe Russo, a visionary at NLECTC-RM, saw the need for the tool and convinced NLECTC to fund its development and provide funding for training professional staff across the country.

© Copyright 2007 by Jim Tanner, Ph.D. All rights reserved.

## Field Search Design

Primary assumptions when developing Field Search:

Field Search would be used in accordance with standard investigative procedures and coordinated with local prosecutors.

Field Search Users would be individuals who were **NOT** CFEs and had **NO** forensic training. Our goals were:

- a. Sharply reduce the load on RCFLs and local police department forensic labs by training non-technical officers in the effective use of preview software.
- b. Provide a tool which could be used by officers to gather timely information to be used in interviews and to make detain/release decisions.

Preserving the target environment was not as important as fast yet through review of critical information.

## Field Search Design

Field Search was designed to sharply reduce the load on forensic labs, maximize field triage of computer devices, and secure admissions by suspects.

1. **SPEED.** The goal is to be in and out of an offender's house with a complete report in less than 30 minutes.
  1. It can collect all data for routine preview exam of an 80GB drive in about 2 minutes.
  2. Data is organized for fast "drill down" review.
2. **EASE OF USE.** We assume the user has **NO** forensic training, and may even have limited computer experience.
  1. Simple interface to expedite exam and inclusion of data in report.
  2. Report constructed dynamically during the exam so the officer is done when (s)he leaves the offender's location.
  3. Runs in a Windows® environment. – we avoided Linux / DOS / PE on purpose.
3. **FLEXIBLE.** While designed for managing sex offenders, we wanted a tool which could be used for managing other cyber criminals as well.
  1. URL histories are generic.
  2. Powerful word search ability.

## Field Search Design

4. **FOCUSED.** The software focuses on those elements of an offender's computer use which maximize containment and preview capability:
1. Automatic URL history detection and extraction for all 4 popular browsers.
  2. Finds all logical images in key formats (JPG, PNG, GIF, BMP).
  3. Finds all multi-media files in formats selected by User.
  4. Conducts word/phrase search at officer's discretion.
  5. Officer can choose to add additional tasks which require more time:
    1. Header search for renamed images.
    2. Scan free space for orphaned URL records.
  6. Generates a complete report in the field.
  7. Exports reference data on all found objects (except images/videos) to an Excel® file.

© Copyright 2007 by Jim Tanner, Ph.D. All rights reserved.

## Field Search Design

5. **MINIMAL FOOTPRINT.** We leave as small a footprint on the drive as possible. We know the minimum footprint Field Search leaves. Most of the changes on the drive are a result of functions built into Windows' operating system. The actual footprint is determined by the state of the computer and the actions taken by the examiner.

Knowing the minimal footprint assists forensic labs **IF** the case is referred on new charges. Minimal impact includes:

1. Additions to the Pagefile and PreFetch/SuperFetch folders.
2. Changes or additions to system event logs.
3. Potential creation of link files if data or reports are saved to removable media..
4. Potential creation of temporary files associated with logs of examiner activity and digests of information preexisting on the hard drive.
5. Depending on what is run, it may change last access date on **FOLDERS** on the drive (but not in the report). A work-around is provided.
6. If User views artifacts in other than "FS native mode", it will change the Last Access Date of the file viewed on the drive (but not in the report).






© Copyright 2007 by Jim Tanner, Ph.D. All rights reserved.

## Who Has Been Trained In Field Search?

- Probation and Parole Departments in 29 States & the District of Columbia
- Two day “hands on” class funded by NLECTC, APPA and other agencies.



## Six Step Process For Probation/Parole

- Set appropriate conditions.
- Catalogue the system (**winaudit.exe**). 
- Examine Registry (**USBDeview.exe** & **ERUNT.exe**)  
- Examine computer for historical use (**FieldSearch.exe**)
  - Goal is to gain info for Tx Team.
- Install monitoring software. (requires a license for each computer)
  - Set monitoring parameters in accordance with case information and findings.
- Wipe free and slack space (**Cleaner.exe**). 
  - Increases chance of proving violation if future problems found.

Departments should establish procedures for use.

**Need For Computer Monitoring While Under Supervision**

Behavioral Indicator	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**

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

LOW-MOD: Active user of porn: Actively seeks images via web pages. – OR – More than 1 hour per month but less than 10 hours a month spent viewing porn.

MODERATE: Collector behavior: Actively seeks through file sharing or catalogues material. – OR – More than 10 hours a month but less than 30 hours a month viewing porn.

MOD-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 porn.

VERY HIGH: Promoter or commercial behavior: Produces or distributes child porn.

© Copyright 2007 by Jim Tanner, Ph.D. All rights reserved.

**Popular Management Software Comparison**

Application	Advantages	Drawbacks	Cost
Cyber Sentinel® Securitysoft.com	Blocks Captures Violations Time Controls Email Alerts	Proprietary Lists Must go onsite to review	\$40 One-time fee
CSWeb® Securitysoft.com	Remote Control Blocks/Captures Viols Time Controls Email Alerts Pricing	Proprietary Lists (can exclude terms however)	\$40 first year \$12 all other years
Spector Pro® Spectorsoft.com	Captures Robustly Time Controls Email Alerts	Must go onsite to review	\$100 One-time fee
E-Blaster® Spectorsoft.com	Captures Email Reports/Alerts Remote Adjustments	Reports daily Captures limited Additional fee for remote installation	\$100 One-time fee
Impulse Control® Impulsecontrol.net	Remote Control Captures/Alerts/Reports Bio-ID Time Controls	Cost	Agency: \$10/mo Offender: \$25/mo

© Copyright 2007 by Jim Tanner, Ph.D. All rights reserved.