



Lightspeed  
Total Traffic Control

INFORMATION PAPER  
AUGUST 2009

# Forensics:

Identifying, Investigating, and Prosecuting  
Sexual Misconduct in Your School

**LIGHTSPEED**  
— SYSTEMS —

Your partner for safe online learning environments

## Table of Contents

Introduction.....	3
Introduction to Forensics .....	3
Predators in Schools .....	4
Profile of a Predator .....	4
Acceptable Use Policies .....	5
Network Set-Up .....	6
IP Address .....	6
Reporting .....	7
Backing up Data .....	7
Warning Signs .....	7
First Steps: Before Forensic Investigation .....	8
Next Steps: During Forensic Investigation .....	8
Review network history .....	8
View user computer .....	8
Image search.....	9
Deleted file retrieval.....	9
Swap file retrieval.....	9
Software tools .....	9
Gather additional non-computer information .....	10
Create a comprehensive report.....	10
Last Steps: After Forensic Investigation.....	10
Lightspeed Solutions.....	11
Lightspeed Systems Forensics Policy .....	12
About Lightspeed Systems .....	12

©2009 Lightspeed Systems

## Introduction

Are your school computers being used in ways that violate Acceptable Use Policies? Probably.

Do you have time to investigate every instance of someone sending personal emails or conducting personal business using school resources? Probably not.

But you have an obligation to both identify and be prepared to prosecute serious, potentially dangerous, infractions of your policies. Nowhere is this more true than in the case of sexual predation.

When school resources are used to find pornographic materials, conduct inappropriate relations with minors, or otherwise create a sexually volatile environment, it is imperative that you have the tools to identify a problem; the proper procedures to address the problem; and the knowledge to conduct a forensic investigation (or preserve evidence for someone else to conduct such an investigation).

In this paper, we will discuss how to create Acceptable Use Policies that both deter such behavior and make clear the violations; how to utilize network activity reports to identify suspicious behavior; and how to collect the evidence you need to suspend, terminate, or even prosecute the violators in your school district.

## Introduction to Forensics

When most people think of forensics, they picture crime scene investigators closely inspecting a scene for evidence, such as fingerprints and DNA. Computer forensics takes the same approach (procedure, scrutiny, discipline) and applies it to digital evidence.

Computer forensics is defined as:

*The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.<sup>i</sup>*

The word *forensic* means “pertaining to, connected with, or used in courts of law”<sup>ii</sup>; as such, one of the critical elements in computer forensics is the proper collection, handling, and presentation of evidence so it stands up under legal scrutiny.

Computer forensics technology makes it possible to retrieve and view data from a computer quickly and accurately. Even deleted files and data can usually be retrieved from a system. And there are forensic tools available today that enable the network administrator to view all pictures and information on a computer on the same subnet in less than fifteen minutes.

## Predators in Schools

While the application of computer forensics may be necessary for other activities, this paper focuses on the use of forensics technology to identify and prosecute sexual predators within schools.

Certainly, most teachers, administrators, and school staff work with students for the right reasons: because they want to help young people achieve and excel; because they desire to pass their own learning along; because they feel compelled to instruct and assist and coach and inspire. However, unfortunately, schools are also a perfect place for sexual predators to lurk: near their prey and in a naturally trusted position.

While up-to-date national statistics are unavailable, a compilation of available research in 2004 suggests that nearly 10 percent of students will be the subject of sexual harassment during their school careers.<sup>iii</sup>

### Profile of a Predator

Who are these sexual predators within schools? Often, they are the people who you would least suspect: white collar professionals with families who attend church and are well-liked. These predators are men and women who lack impulse control and are often triggered into sexual misconduct as a stress response to a bad situation, such as a death in the family, a financial problem, or a divorce.

Though a profile of a typical offender certainly shouldn't be employed to ascertain guilt or innocence, it can be useful when trying to get a picture of a possible culprit. In general, sexual predators fit the same profile as pornography addicts: white collar professionals, males, age 40-55, somewhat religious, married, with children.

Within schools, predators are often not easily identified as a danger to children, and are often celebrated within their professions.<sup>iv</sup> The 2004 survey of available research found that while teachers and coaches are the most commonly-held positions for predators within schools, it is not limited to those job titles.

<b>Percent of targets by offender's job title<sup>v</sup></b>	
<b>Job Title</b>	<b>Percent</b>
Teacher	18
Coach	15
Substitute Teacher	13
Bus Driver	12
Teacher's Aide	11
Other	10
Security Guard	10
Principal	6
Counselor	5

In short, sexual predators within schools are not always easy to identify. They are the people you would least suspect, who first cross the line with inappropriate behavior such as:

- Downloading or bringing pornography onto school systems
- Conducting inappropriate communications with students
- Harassing other employees or other people outside the school system

## Acceptable Use Policies

An essential element in any school's technology plan is an Acceptable Use Policy (AUP) that clearly defines how, when, by whom, and for what purpose a school's technological resources are to be utilized. The policy should also clearly state what the consequences of infringement are. For all students, teachers, and staff who use the school technology, an updated Acceptable Use Policy should be read and signed every year. Since the policy should be able to serve as a legal document, a school attorney should also review it.

**BEST PRACTICE:** Make sure an updated, signed Acceptable Use Policy is on file for every student, teacher, and staff—annually.

An Acceptable Use Policy should include at least:

**Introduction** – A listing of the various technologies available in the school and to which this AUP applies. Also, a description of the goals and educational philosophies that the technologies in your school support. And finally, a discussion of what the AUP itself is designed for and what it covers.

**Usage Policies** – A discussion of various policies surround the use of technologies, including when technologies are to be used by students and staff as well as for what purposes; the issues of copyright and plagiarism as it applies to the Internet; netiquette and appropriate online behavior; privacy policies; and an explanation of the various filtering and monitoring devices that are used on school computers.

**Acceptable Uses** – Specific examples of acceptable uses of school technologies, computers, and the Internet.

**Unacceptable Uses** – Specific examples of UNACCEPTABLE uses of school technologies, computers, and the Internet. This should include a discussion of pornographic images, sexual content, and sexual misconduct.

**Consequences** – A discussion of the expected consequences of policy infringement, for both students and staff.

**Liability** – A disclaimer, freeing the school from liabilities that may arise.

**Acceptance** – Signature and date for each user of school technologies, acknowledging that they have read and understood the policy and agree to follow its guidelines.

Acceptable Use Policies are essential documents, designed to help students and staff understand their expectations and to help the district and administrators impose consequences, or pursue prosecution or termination, for inappropriate use. However, often Acceptable Use Policies are unused, vague, or not updated. As the IT director or administrator responsible for these technologies, you should advocate for a school board policy that requires annually updated, signed Acceptable Use Policies for all users.

## Network Set-Up

How your network is set up and managed is the first step to enforcing any Acceptable Use Policy. Before any inappropriate behavior is identified, before an administrator tasks you with looking into a user's activity, before you begin anything related to computer forensics, it is essential that your network be set up and managed in such a way that individual users can be identified, reporting is unbiased, and data is readily available.

### IP Address

If you suspect activity that violates your AUP, identifying the person doing the activity should be restricted to having TCP/IP information and two eye witnesses or video confirmation.

**BEST PRACTICE:** To solidify your case and tie a user to a particular computer, you should provide eye witness testimony from two people who saw the user using the machine in question, or video evidence.

Should an investigation move forward, it is a best practice that you have your DHCP settings configured so that you can testify to having an IP address that is considered static. In order for a DHCP address to be considered static, the lease time needs to be at least one year. With anything less than a static IP address, and any time period less than one year, your testimony about activity on a certain computer will be considered uncertain. Once you discover activity that you want to investigate, it is acceptable to put a static IP address on that machine, or to create an exception in the DHCP scope for the current IP address. Use of a username or login instead of an IP address can lead to questioning and scrutiny of the servers that give those logins out, including their maintenance and patches and usage.

**BEST PRACTICE:** Use static IP addresses to identify computers and users rather than Active Directory/LDAP settings and logins.

## Reporting

As a best practice in general, but also to avoid any show of bias during an investigation or trial, it is important that reporting of user activity, browsing, searching, and more be conducted based on all users, and be both comprehensive and consistent. A reporting history that shows comprehensiveness will stand up better against a charge of bias against a single individual. By consistently performing the same reports in the same ways, using the same naming conventions, you will be able to more easily assert objectivity and confidence in your processes.

## Backing up Data

Often, you don't know what you're looking for until too late. For example, a search for "giggling girl" wouldn't be flagged as suspicious. But, should an investigation open later, that very search could be valuable evidence of searching history and behavior patterns. Therefore, it is important to back-up and store all data in case it is needed for more comprehensive reporting and analysis later.

**BEST PRACTICE:** When a teacher leaves their position, save, date, and file their hard drive for at least two years—noting chain of custody.

## Warning Signs

Regular review of user activity is critical to maintaining the health and appropriate use of your network, and to enforcing Acceptable Use Policies. When it comes to watching for suspicious activity that could indicate sexual misconduct or predation, there are a few specific things to pay close attention to.

**Suspicious Traffic** – Are users regularly going to, or attempting to go to, certain sites (such as pornographic) that indicate inappropriate activity? Are certain users utilizing the school computer or network for unnecessarily long periods of time, or at odd hours?

**Searches** – Suspicious or blocked searches of a possibly sexual nature (such as "naked boy" or "naked girl") may be a red flag that should warrant further investigation.

**Blocked Content** – A review of blocked content will, in most cases, illustrate things other than predatory activity. However, keeping an eye on blocked content can reveal repeated attempts by a single user to access inappropriate content.

**Instant Messaging** – As demonstrated in the profile, sexual predators lack impulse control. High-volume messaging, particularly between a teacher and student, should be reviewed.

**Email** – There are many legitimate reasons for students and staff to communicate via email. However, should email between a staff and student be reported as top email senders/receivers, it should be further investigated.

## **First Steps: Before Forensic Investigation**

For your protection, the protection of the district, and the protection of the case (should it come to that), it is important to follow certain steps in the event that sexual misconduct is suspected.

1. Do not panic. Regardless of the infraction, don't respond with an emotional reaction and do not take immediate action against the suspected abuse/abuser.
2. Bring your concern to administration. The way the suspected misconduct is handled should be decided by administrators. Take the information you have to them, and let them decide the course of action.
3. Ask for permission in writing to investigate further. To protect yourself, and show a proper chain of command, should the administrator instruct you to investigate further you should request that permission in writing, and signed and dated.

<p><b>BEST PRACTICE:</b> If from your initial review, you suspect child pornography: Stop and notify a law enforcement agency.</p>
--

## **Next Steps: During Forensic Investigation**

### **Review network history**

Once you have been told (and given written permission) to move forward with an investigation, you can begin by delving more deeply into the individual's browsing, searching, messaging, emailing, and other online behaviors. View all available reports and compile any information that shows inappropriate behavior or a pattern of behavior. Create PDF documents of all reports you decide to retain.

### **View user computer**

Viewing the user's computer can provide significant information about the types of activities they have been doing with school resources, from downloading and storing inappropriate images to engaging in inappropriate communication. Because the computer in question is school property, there should be no expectation of privacy, based on a signed Acceptable Use Policy.

When looking at a computer and investigating its contents, it is important that you use the proper tools and procedures so as not to alter files, corrupt evidence, or bring into question your techniques.

Mathematical hashing is a process by which large quantities of data (such as file contents) are translated into a string of integers. Hashing allows you to compare file contents easily: if the hash numbers match, the files are identical and have not been altered. It is essential that all evidence have a hash value that both the prosecution and defense can agree on.

### **Image search**

One of the most likely things you will search for is image files. With regard to image files, many courts use a Dost Test<sup>vi</sup> to determine if a given image is considered “lascivious” under the law. This test judges images by six factors:

- Whether the genitals or pubic area are the focal point of the image;
- Whether the setting of the image is sexually suggestive (i.e., a location generally associated with sexual activity, such as a bed);
- Whether the subject is depicted in an unnatural pose or inappropriate attire considering her age;
- Whether the subject is fully or partially clothed, or nude;
- Whether the image suggests sexual coyness or willingness to engage in sexual activity; and
- Whether the image is intended or designed to elicit a sexual response in the viewer.<sup>vii</sup>

While context is extremely important in judging an image, this test can help you determine the appropriateness of images as you review a hard drive.

### **Deleted file retrieval**

Generally, when files are deleted they leave enough information to be able to put them back together. A single piece of information can be found in up to seven different places on a hard drive. Retrieving deleted information from a hard drive is most successful sooner rather than later.

### **Swap file retrieval**

Swap files are spaces on a hard disk used as virtual memory. These files are stored in a computer’s upper memory and often house information such as print jobs and key strokes. Swap files can be lost when a computer is turned on or off. By unplugging the computer, swap file data remains on the hard drive—giving you up to one-third more information. When investigating a laptop, it is a best practice to remove the battery in addition to unplugging the machine.

### **Software tools**

Software tools can help you quickly and easily view the contents of a user’s hard drive, including information that was deleted. It is essential that an investigation into a hard drive does not corrupt or alter any files on the hard drive, so using the proper tools and procedures is important.

**Helix software** – Helix 3 Pro from e-fense offers both a bootable forensically sound environment (to make forensic images of a device and search file systems for certain data and file types) as well as a live side (to make forensic images of all internal devices and physical memory, as well as to determine if disk encryption is turned on). Find out more at <http://www.e-fense.com/helix3pro.php>

**EnCase software** – EnCase Forensic from Guidance Software gives you the ability to image a drive and preserve it in a forensically sound manner, utilizing a court-recognized Logical Evidence Format. Find out more at: <http://www.guidancesoftware.com/default.aspx>

**BEST PRACTICE:** If you use only NIST (National Institute of Standards and Technology)-approved devices and software, you won't have to provide testimony on HOW the tool works, just what it discovered.

### **Gather additional non-computer information**

In addition to computer and network evidence, there may be additional information to help create a solid case around an individual. If available, gather any video of the user (using a specific computer at a specific time, performing unusual acts, entering the building at odd hours, etc.). Also, gather any eye witness testimony. In addition, any building or entry/alarm records can help to build a case against an individual who used school resources during off-hours.

### **Create a comprehensive report**

Next, you need to pull everything together into a comprehensive report that clearly and objectively presents the inappropriate behavior the individual was engaged in.

To create the most compelling report:

- PDF everything in subject, date, and time formats
- Show all graphics (or if there are more than 100, show a sampling of the most egregious)
- State only facts; no opinions
- In addition to details of the misconduct, provide details of your own process of discovery and investigation

### **Last Steps: After Forensic Investigation**

Should the case go to court, it is important that you can testify on your involvement in the process of data collection. Before presenting evidence, you will be asked to establish your credibility as a professional.

In addition to the tips throughout this white paper for ensuring proper process and evidence integrity, we offer these tips:

**Know your stuff.** Review your notes so that your actions and thought-processes are able to be recollected quickly and easily, despite the fact that events about which you are testifying might have happened years ago.

**Be an expert.** It will be more difficult for the defense to question your expertise and skills if you present yourself as an expert. Certifications and publications can boost the reliability of your testimony.

**Keep it simple.** When describing complex technical processes or concepts, it is important to use language that is easy to understand. Stick with two-syllable words, and an 8<sup>th</sup>-grade level vocabulary.

**Be honest.** The worst thing that can happen during your testimony is that you look like a liar. The best answer to a question during cross-examination is the honest answer.

## Lightspeed Solutions

Lightspeed offers a suite of products designed specifically to help schools manage, secure, filter, and optimize their networks more efficiently and effectively.

To identify policy infringements, investigate issues more deeply, and possibly prosecute cases, you need in-depth information about network traffic and user behavior, at your fingertips. Our solutions give you access to comprehensive information about who, when, where, and how your network is being utilized, so you can adjust Acceptable Use Policies, change allowed usages, review problems and troubleshoot issues, and plan for ongoing needs. You can see high-level overviews, and then drill down for detailed information. All reports can be viewed and configured locally or remotely, printed to a PDF file, exported to a CSV file, and automatically emailed.

**Total Traffic Control** provides a single, comprehensive solution for managing and ensuring your school network's usage, health, and security.

With Total Traffic Control, you can be alerted to potential problems and investigate them more easily with reports such as:

- *HR Report*
- *Top Suspicious Search Engine Queries*
- *Blocked Search Queries*
- *Blocked Content*
- *Top Email Senders/Receivers*

In addition, Custom Reports give you in-depth information on exactly the data you wish to capture, allowing you to create reports on individual users, for specific information, or over specific date ranges.

Total Traffic Control also offers a Backup & Restore function, making data archiving easy. The primary purpose of the Backup and Restore operations of the Statistics Database is to accommodate archiving of aged network traffic statistics. If necessary, these 'Backup' files can be restored in order to generate or recreate traffic reports beyond the normal scope of the regular statistical recording time frame. Database backups are performed, automatically at 2am, every 7 days and will be kept for 4 weeks, by default.

**BEST PRACTICE:** To create a lifetime record, store your statistical database in a different location.

## **Lightspeed Systems Forensics Policy**

Lightspeed Systems has created network reporting in order to assist school districts with identifying all Internet activity traveling in and out of the district-owned network. Many reports have been created to assist HR investigations in K-12 education settings. Lightspeed has tested the accuracy of all reports at a forensic level, which proves that what is on a report is an accurate accounting of what was committed on a specific computer.

Lightspeed employs a certified forensic investigator that can demonstrate the validity of the reports obtained. Lightspeed can offer this as a professional service on a cost recovery basis if needed.

## **About Lightspeed Systems**

Lightspeed Systems Inc., founded in 2000, develops comprehensive network security and management solutions for the education market. We are committed to helping schools operate their networks effectively and efficiently, so educators can provide safe online teaching and learning environments.

Our software is used in more than 1,000 school districts in the United States, the United Kingdom, and Australia to protect more than 5 million students. For the past two years, Lightspeed Systems has been recognized on the Inc. 5,000 list as one of the fastest-growing private companies.

[www.lightspeedsystems.com](http://www.lightspeedsystems.com)

---

<sup>i</sup> [http://www.us-cert.gov/reading\\_room/forensics.pdf](http://www.us-cert.gov/reading_room/forensics.pdf)

<sup>ii</sup> <http://dictionary.reference.com/browse/forensics>

<sup>iii</sup> <http://www.ed.gov/rschstat/research/pubs/misconductreview/report.pdf>

<sup>iv</sup> <http://www.ed.gov/rschstat/research/pubs/misconductreview/report.pdf>

<sup>v</sup> <http://www.ed.gov/rschstat/research/pubs/misconductreview/report.pdf>; Source: Shakeshaft, 2003; AAUW, 2001

<sup>vi</sup> From the case, United States v. Dost, 636 F. Supp. 828 (S.D. Cal. 1986).

<sup>vii</sup> <http://ilt.eff.org/index.php/Lascivious>