

## **Michigan Businesses Embrace Computer Forensic Investigations To Protect Themselves**

*With the majority of workers utilizing computers on the job, businesses face major security and misconduct issues that are often stored in those computers. The private detectives at Advanced Surveillance Group in Michigan are assisting business to fight fraud and to detect employee abuses and misconduct by utilizing computer forensic investigations.*

Detroit, MI (PRWEB) January 31, 2006 -- With nearly all business documents and a large amount of business correspondence being generated on computers, more and more Michigan businesses are finding that their computers hold far more information than they thought.

Deleted documents, email messages, web pages visited, uninstalled software applications and many other types of business documents can frequently be found on a computer by a trained computer forensic investigator like those working for Advanced Surveillance Group, Inc., a private detective agency based in Mt. Clemens.

Evidence of employee misconduct, violations of company policies, including but not limited to electronic use policies, viewing and/or creating illicit and illegal material, sexual harassment, racial discrimination, and theft of proprietary information are often discovered in a computer forensic investigation of the subject's P.C., laptop and/or email servers. Frequently we find inappropriate behavior in this type of investigation that would give your client a legitimate reason to terminate the employee or defend their position if they've already been terminated regardless of the original reason.

Worse yet are those employees who engage in the following on their computer:

- Theft of customer information
- Theft of financial information
- Altering financial records (usually done in conjunction with actual fraud)

Additional threats exist on a more frequent basis and result is lost productivity and massive personnel costs like reading/sending personal email, surfing pornography, online gambling, participating in E-Bay related activities, chatting, playing games and creating informal correspondence or files about work that are offensive or in direct violation to company policy that would not exist otherwise.

“We read articles about stock brokerage firms that have been successfully sued for hundreds of millions of dollars because of informal email messages about client activity, or cases involving discrimination or harassment

resulting in the same awards and all of the culpable information was derived from an employees computer utilizing computer forensics.” reports Paul Dank, licensed private detective and owner of Advanced Surveillance Group. “The good news is that we can easily employ this type of investigation to the benefit of the company by using it to locate threats ahead of time, to help defend employers in wrongful termination lawsuit and to catch thieves.”

Computer forensics is the process of gathering evidence from a computer or computers in a forensically accurate and verifiable manner. Aside from having the specialized hardware and software to get to the data, it is vital to have an investigator to analyze what they find and peel back layer after layer to get you complete

results.

With so many computer consulting firms offering forensic work, one may ask, why should I hire a licensed private investigator trained in computer forensics to do this type of work rather than IT staff or outside computer consultants?

To answer that, there are a couple of reasons. In Michigan, as the client of a private detective, you have the same level of confidentiality that you benefit from with your physician or attorney, meaning, even if the evidence we locate is harmful or if you simply elect not to use it, no other third party can gain access to it or use it against you.

Further, IT staffers do not think or act like investigators. They are not trained to work with evidence nor are they knowledgeable in how it must be handled to be preserved as evidence usable in court. IT staffers are not trained in legal considerations associated with computer forensics. In addition, the evidence that the private detective finds often turns into additional non-computerized leads that need to be followed up on to make the evidence complete, and the IT staffer is simply not capable of doing this work.

The use of forensic specialists and a proactive approach to incident handling will improve organizational resilience and reduce the would be costs of expensive legal battles.

by Paul Dank, Licensed Private Detective

###

### **Contact Information**

**Paul Dank**

Advanced Surveillance Group

<http://www.asginvestigations.com/computer-forensics/>

888-677-9700