

Full-Disclosure: Re: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

## Re: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0082.html>

---

**From:** Steve Kudlak (*chromazine\_at\_sbcglobal.net*)

**Date:** 09/04/05

Date: Sat, 03 Sep 2005 22:45:18 -0700

To: dave kleiman <dave@isecureu.com>

dave kleiman wrote:

>Steve,

>

>Inline..

>

>

>

>>Hate to play alwyer here but doesn't all of this get shot down by 3rd

>>Circuit Federal Court of Appeals decisions regarding the FBI's

>>Innocent Images project? It basicly shot down the concept of "you

>>clicked on a chold porn link therefore you're guilty."

>>

>>

>

>Well that applies to when it is determined that it was innocent. This could

>be via pop-up, trojan, or malware of some kind.

>

>

>

>

>

>>This is all enshired in Federal

>>Cases. No one must admit that a good prosecutor can indioct a ham

>>sandwich and all that. But overall that doesn't happen.

>>Now Federal Prosecutors and Investigations staffs are very good at

>>sort of getting warrants and raiding someone's house or business and

>>going thru everything. But if the person doesn't scare and cop to

>>something they never did, then federal prosecutors generally have to

>>back off in cases where it is just things accumulating on disks etc.

>>

>>

>

>Well they do not usually prosecute ham sandwiches, BLT's maybe.

>

Re: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Full-Disclosure: Re: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

>I love how everyone is quick to say things just magically accumulated on  
>their H/D. However, they tend not back of when a file structure is found  
>with hundreds of images, often burned to CD's.

>

>

>

>>Futhermore in

>>states with a high privacy expectation like California there is a good

>>reason to say "We don't go through our customers data looking for

>>things out of the ordinary". One might argue it to be different it

>>were one's employees. However if you are offering a primo privacy

>>service then you can legitimately scrub disks as a part of the biz

>>plan.

>>

>>

>

>Well that may be, of course you missed the beginning of these threads, where

>Mr. Combs suggested after discovering contraband on and employees H/D, to

>make a copy of it take the copy to the companies attorney. Wipe the original

>and "best course of action is to purposefully falsify the record of the

>company's response to the incident"

>

>The full threads can be read here:

>

><http://seclists.org/lists/security-basics/2005/Sep/subject.html>

><http://seclists.org/lists/security-basics/2005/Aug/subject.html>

>

>

>

>

>>Much of Law Enforcement and their Public Providers of services

>>depends on scaring people and businesses into good behavior when it is

>>neither necessary or ethical. My suspicion is that one can ignore this

>>tactic if one wishes as one is reasonably careful.. I am sure that

>>people will be offering "Computer Forensics Services" to find the

>>scary things on your compnys disks for \$500 a pop but no good reason

>>one has to engage in such silliness.

>>

>>

>

>

>Yes that crazy scaring people into good behavior..... Oh wait that is

>right only reasonably prudent people follow the law, criminals tend to not

>care if there is law against something, they are not scared into not

>committing crimes, that is why they are criminals.

>

>Kind of like the lawlessness that is occurring in the situation you

>mentioned below. Some people would say that the devastation has turned

>these people into criminals. Although, the reality is the people committing

>the crimes are the same ones that were committing them before the

>devastation.

Re: [Full-disclosure] RE: Computer forensics to uncover illegal internet use



Now if one talks to Federal Prosecutors they will tell you that they feel comfortable with their "Vacuum Cleaner" approach. They feel if they do go and get everyone's questionable stuff and go through it, then one will be able to determine how many folks had things accumulating on their disk and how many actively collected it etc. Now interestingly with the Third Circuit's Decision which is close to rock solid at this point in precedent, people like journalists would sort of get wide discretion especially if they were working on stories and doing investigations etc.

Two other things come in here. In both the US Ninth Circuit and Upper Level Courts of British Columbia it has been held that one can not commit crimes against "virtual children" or "animated descriptions of children etc". This means the general belief in liberal democracies that "thought crimes" are questionable is beginning to be enshrined in code and precedent. I am pretty sure this is well embedded in North American Culture and is apt not to go away even with the idea, darfe I say spectre two very conservative reversalists judges on the Supreme Court. Note I have not had time to study how things work in the EU or even Australia.

Now technoculturally what this may eventually provoke is the use of high grade encryption by more people. Right now I know even artists who have become more technologically savvy and who encrypt things even when legal code is on their side overall. In the 1970s and 1980s there were a number of legal razzlements of artists who used their children as nude models no matter how innocent. This went too far and eventually what got established is the concept that "simple nudity is not obscene". It is interesting because artists are not usually seen as users or consumers of security products and things like encryption.

Anyway this is all very interesting and we do live in interesting times. So it will be interesting to see how this will go and whether the business idea of trying to safe from all possible wrongdoing or perceived wrongdoing will win out overall. I know lots of vendors and security consultants have been hoping that "porn protection" would turn into a lucrative field but so far it doesn't compare to virus and malware protection.

Interestingly in artist circles the whole imaging thing has turned into "sousveillance" and artists have been having way too much fun turning the cameras back on the people who usually use them. It is interesting that people like Sudo Chiles House who was one of the first people to install a "cam" which in her case was a 35mm camera that took pictures regularly of her bedroom is all but forgotten in the modern installation of cams in various public and private spaces. Note the UK and places in Florida have been very much into the "you are being watched" theory of crime control. I also have heard tales of "spy camera destroyers" who have been running around spray painting cameras but I think that is not widespread at this point. Hmmm, indeed these are interesting times. whether it is a blessing or a curse is an open question.

Full-Disclosure: Re: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Have Fun,  
Sends Steve

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>