

## RE: Advice regarding servers and Wiping Drives after testing

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-09/msg00094.html>

---

- *From:* "William Holmberg" <[wholmberg@xxxxxxxxxx](mailto:wholmberg@xxxxxxxxxx)>
  - *Date:* Wed, 12 Sep 2007 11:18:39 -0500
- 

Dave,

<Note- the links from your page on Infragard "Zip | PPT | Handout PDF | CD Active Links PDF" Do not work, although Mr. Bejtlich's links do- I'd like to get your data for future classes>

I looked up my notes on that day, to verify my memories of the presentation, and to answer your question...

Well, yes and no...

The first example, the instructor clearly stated that the drive had been overwritten 0's, and supposedly recovered a file in the lab (the recovery process was not shown), in this case a .jpg which was partially (3/4's) viewable. He remarked the technique would remain undisclosed, but that it was time intensive and expensive, yet still used regularly. He did not say it wasn't ESM either, so perhaps that is what it was. I paraphrase him by the quote "Even when the drive has been overwritten with 1's and Zeroes we can often get evidence with this new procedure". Frankly, I remember him saying it having something to do with magnetic signatures, differentiation and time (age) of magnetic signatures, if that makes sense.

The second example the drive was formatted and partitions deleted, and data was recovered successfully on that example, but there was a third demonstration where some files that were overwritten with another type of file, and it was presented to us (understand, we were viewing the process remotely, and there was no way for me personally to verify exactly what was really occurring on the other end, but we had no reason to doubt the veracity of the claims) that the overwritten files were recovered immediately after the overwrite. I do remember that I had questions about that particular procedure because in that case the computer had not been restarted, but was still running. I had thought perhaps some NVRAM or swap file was involved in the recovery, but time did not permit us to ask all the questions I and the attendees had for the team presenting. The examiners referred to the users method as a virtual "flashpaper" technique where a small directory was overwritten with other innocuous files by the suspect through a software package which responded to a Hotkey.

RE: Advice regarding servers and Wiping Drives after testing

We were also given the impression that the third recovery technique was quite new, perhaps even experimental, and that the types of files recovered were limited by both their type as well as the types of files replacing/overwriting the existing files. I was told it had something to do with the way the files were altered which allowed restructuring of what had changed, but there were no technical specifics given.

I'm sorry I don't have more on it. If we are successful in getting more funding for the DOJ classes I will press the issue in the next semester with others involved to see if I can get some more specific info on those aspects.

Specifically though, you are correct that in the formatted example, the drive had not been "shredded" and completely overwritten with a program intended to subvert any recovery, although the examiner did allude to it being "extremely more difficult" once that was done, though the implication was that it was not impossible. He also did show how to tell that certain programs had been used (on another drive) to totally remove potential evidence, which was also interesting, and sounds like it is similar to what your class accomplished in San Diego.

So, specifically, Ansgar is likely quite correct that in a case where the drive has been shredded by overwriting in that manner that no data can be recovered easily— but we were given the impression that it had just been done, though it was possible that was a limited ESM method.

I do not claim personal expertise in this area, as I mentioned, but I do believe that most people in the class came away with the impression that it could be done, but there was mention of a cost to benefit ratio, and even admissibility of the evidence. For instance, if the drive was purchased as a refurbished drive from any vendor, it is likely the agencies would rarely try to ESM for evidence because no matter how successful they may be, a shrewd lawyer could quite easily get a jury to have reasonable doubts about where the data recovered actually came from.

I will ask our director to reschedule this presentation again and be sure to ask some more pertinent questions next time to see where exactly the parameters of the presentation begin and end. If there are other definitive articles, etc. you all know of, please let me know as I would love to expand on this topic in the classes. Perhaps we could even setup a remote presentation with some of you— though I warn you the class pays poorly!

:0)

All the best,

Bill

-----Original Message-----

From: dave kleiman [<mailto:dave@xxxxxxxxxxxxxxxx>]

Sent: Wednesday, September 12, 2007 9:08 AM

To: security-basics@xxxxxxxxxxxxxxxx

RE: Advice regarding servers and Wiping Drives after testing

RE: Advice regarding servers and Wiping Drives after testing

Subject: RE: Advice regarding servers and Wiping Drives after testing

Bill,

I think you are mistaken. I attend and teach labs at most of the forensic events yearlong including the FBI InfraGard National Conference ( <http://tinyurl.com/24vuj8> ). As a matter of fact, last month at the HTCIA International conference in San Diego, part of my class demonstrated how to identify the traces of different types of erasure programs. These were single random and/or zero passes. You can download it here: <http://tinyurl.com/35mbc9> . I have NEVER seen or heard of a demonstration or tool, outside of an ESM Electron Scanning Microscope, that would recover the data after being "wiped". Perhaps you are thinking of after deleting partitions and/or formatting several passes??

Dave

Respectfully,

Dave Kleiman – <http://www.davekleiman.com>  
4371 Northlake Blvd  
Suite 314  
Palm Beach Gardens, FL 33410  
561.310.8801

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx  
[mailto:[listbounce@xxxxxxxxxxxxxxxxxxxxx](mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx)] On  
Behalf Of William Holmberg  
Sent: Tuesday, September 11, 2007 17:36  
To: Ansgar –59cobalt– Wiechers; security–basics@xxxxxxxxxxxxxxxxxxxxx  
Subject: RE: Advice regarding servers and Wiping Drives after testing

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxxx

RE: Advice regarding servers and Wiping Drives after testing

RE: Advice regarding servers and Wiping Drives after testing

[mailto:listbounce@xxxxxxxxxxxxxxxxxxxxx]

On Behalf Of Ansgar -59cobalt- Wiechers

Sent: Tuesday, September 04, 2007 1:03 PM

To: security-basics@xxxxxxxxxxxxxxxxxxxxx

Subject: Re: Advice regarding servers and Wiping Drives after testing

On 2007-09-01 gjgowey@xxxxxxxxxxxxxxxxxxxxx wrote:

- > A since pass with all zero's really won't protect your data from being
- > recovered by more advanced data recovery software let alone alone
- > hardware.

I'd like to see a single case where someone was able to recover data from an overwritten harddisk, even after a single pass with zeroes.

\*\*\*\*\*

Hi,

No doubt you are an intelligent and well educated person in these fields, and probably have many areas of expertise more proficient than mine. I do have to state however, and nearly any Infragard member can tell you, the FBI uses tools that accomplish this on a regular basis.

I have no doubt other agencies do as well. We have had demonstrations of it remotely in a class I help instruct, SAFE computing for Law Enforcement and Non-Profits (SAFE is Security And Forensic Education) at Metro State University of Minnesota, MCTC campus.

My .02...

-Bil