

Forum:[Hack Forums](#)

Thread: [data shredder vs. a complete reboot?](#)

mrhack - December 9, 2017, 8:15 pm

I'm trying out Avast Premier and saw that it has a "data shredder" feature. It can shred selected files, shred whole drive, and shred deleted files. The "shred whole drive" shreds an entire drive and all the data in it. My question is, wouldn't a complete reset/factory setting of the drive be the same thing or not since "system restore" may still be possible?

+mK - December 9, 2017, 8:33 pm

There are tons of softwares that act as "data shredders", or wipers. They overwrite the data with random data so that the information cannot be professionally recovered.

datguy.dev - December 10, 2017, 7:28 pm

(Dec 9, 2017 09:15 PM)mrhack Wrote: [\[CITE\]](#) I'm trying out Avast Premier and saw that it has a "data shredder" feature. It can shred selected files, shred whole drive, and shred deleted files. The "shred whole drive" shreds an entire drive and all the data in it. My question is, wouldn't a complete reset/factory setting of the drive be the same thing or not since "system restore" may still be possible?

With shredding or wiping, you're writing over the sectors on the disk where the data for files are located at a deep bit-level. Windows has an old CMD tool for wiping called "cipher" btw. But resetting or doing a clean install will only format the disk. Where the old information is still there. The OS is simply not aware of it.

As far as the data in restore points. The copies of files are referred to as "shadow copies" in Windows. If restore points are available, then that data can be recovered. I'm not sure restore points are 100% viable in a court of law. There are rules. But they probably could make it work depending on the severity or authenticity of the files etc.

If you want to properly wipe your disk, expect to do a full disk wipe and use a bootable utility like DBAN and do a DoD 3-pass. Shredding a few files is a sloppy process that often leaves some evidence somewhere else on the disk of it's presence or direct information. Like cache or temp files that express the shredded files contents.

NedwonsDrawde - August 3, 2018, 11:31 pm

(Dec 9, 2017 09:15 PM)mrhack Wrote: [\[CITE\]](#) I'm trying out Avast Premier and saw that it has a "data shredder" feature. It can shred selected files, shred whole drive, and shred deleted files. The "shred whole drive" shreds an entire drive and all the data in it. My question is, wouldn't a complete reset/factory setting of the drive be the same thing or not since "system restore" may still be possible?

Factory reset alone is not secure.

- Cincinnatus

mrhack - September 1, 2018, 2:04 am

so if one uses a laptop solely for hacking, could one customize it so that it lacks a restore point (is it possible?). So a factory resetting isn't legitimate? is DBAN a software program? What does DoD 3-pass mean? Is that in relation with the DBAN program?

Is what you said workable in virtual computers as well? Are the things talked about here deemed "ethical" in the ethical hacking world or is it the reverse, but who cares?

(Dec 10, 2017 08:28 PM)datguy.dev Wrote: [\[CITE\]](#) With shredding or wiping, you're writing over the sectors on the disk where the data for files are located at a deep bit-level. Windows has an old CMD tool for wiping called "cipher" btw. But resetting or doing a clean install will only format the disk. Where the old information is still there. The OS is simply not aware of it.

As far as the data in restore points. The copies of files are referred to as "shadow copies" in Windows. If restore points are available, then that data can be recovered. I'm not sure restore points are 100% viable in a court of law. There are rules. But they probably could make it work depending on the severity or authenticity of the files etc.

If you want to properly wipe your disk, expect to do a full disk wipe and use a bootable utility like DBAN and do a DoD 3-pass. Shredding a few files is a sloppy process that often leaves some evidence somewhere else on the disk of it's presence or direct information. Like cache or temp files that express the shredded files contents.

datguy.dev - September 2, 2018, 7:11 pm

(Sep 1, 2018 02:04 AM)mrhack Wrote: [\[CITE\]](#) so if one uses a laptop solely for hacking, could one customize it so that it lacks a restore point (is it possible?). So a factory resetting isn't legitimate? is DBAN a software program? What does DoD 3-pass mean? Is that in relation with the DBAN program?

Is what you said workable in virtual computers as well? Are the things talked about here deemed "ethical" in the ethical hacking world or is it the reverse, but who cares?

DBAN is software you would burn to a CD and boot from. Department of defense 3-pass; google it. DBAN can perform a DoD 3 pass.

Perhaps you should just look into encryption. Make sure that all you are doing is contained within the scope of that which is encrypted. Such as you may use an encrypted volume on your disk. If you cannot keep all that you do within that volume (portable programs, sandboxes etc) than encrypt your entire disk. Honestly, you should be educated on your own foot print and security before doing anything "unethical." Good luck.