

Forum:[Hack Forums](#)

Thread: [Forensics on laptop and securely wiping?](#)

bmurph25 - November 21, 2018, 5:26 pm

I have read a bunch of info on erasing SSD drives and there's a lot that conflicts with one article to the next. What's the right answer as to whether the drive manufacturers SSD tools really erase the drive so that no data can be recovered by anyone?

Is it really to physically destroy the drive which I know is the safest solution? Or do the tools out now really wipe it?

Then if a laptop was used to access sites that shouldn't be accessed, if it was done when connected to VPN, I know the IP is what is looked for, so depending on the VPN provider there would be logs or no logs. If the sites were accessed when not on VPN then if a request for records was made, my ISP's public IP assigned to me would be what's given back in the search result from whoever requested it.

In that case, is the IP address enough to prove that someone did something wrong? I am asking because I've read just an IP isn't enough to prove this, that it requires data whether from a computer, USB drive, or so forth?

If I didn't want to trash the laptop physically, what other information can be retrieved to determine if it was the computer system used to access the websites or services? Is it only the drive, or are there other things such as the MAC address? I would expect the MAC address detected would be the routers/firewalls, but I've also read that getting the MAC address remotely isn't possible?

SIM-1073426 - November 23, 2018, 8:28 am

To be honest, just destroy it. If you want anything on that drive secret then the only secure way to be 100% certain that that data is gone is to physically destroy it.

F.B.I - November 23, 2018, 9:32 am

The only way to make sure all data is irrecoverable is to destroy it. Use a drill and a hammer.