

Forum:[Hack Forums](#)

Thread: [USB FLASH DRIVE Tracking](#)

bigtoymario - June 25, 2019, 4:51 pm

Question if I use a USB flash drive and send it anonymously to someone can the USB Flash drive be traced to my PC?

Does anyone know if it holds any data that someone can access to trace it back to my PC?

I am planning on sending pictures and a text file so I want to make sure I remain anonymous. I want to avoid any tracking or tracing.

970DD0113CD312D7A3F8B5411 - June 25, 2019, 6:02 pm

Fairly certain it is possible to trace it back to you.

If you're sharing photographs, it is a good idea to open them in paint (on a VM) and re-save them to strip any metadata.

CyberStrike - June 25, 2019, 6:18 pm

All this for a few pictures and text files? Well the simple answer is yes, both the files will contain data which can be used to identify both the computer, location (pictures have this), camera used or scanner, also artifacts are found on the computer in regards to USB devices. This can all be done forensically now being this sounds fishy I am not too comfortable with going too much further, just in case this has to do with terrorism or something to do with kids. If what you are doing has to do with anything I mentioned in the previous sentence, then well I doubt anyone would help.

bigtoymario - June 25, 2019, 6:47 pm

(Jun 25, 2019 06:18 PM)CyberStrike Wrote: [\[CITE\]](#) All this for a few pictures and text files? Well the simple answer is yes, both the files will contain data which can be used to identify both the computer, location (pictures have this), camera used or scanner, also artifacts are found on the computer in regards to USB devices. This can all be done forensically now being this sounds fishy I am not too comfortable with going too much further, just in case this has to do with terrorism or something to do with kids. If what you are doing has to do with anything I mentioned in the previous sentence, then well I doubt anyone would help.

It has nothing to do with kids or terrorism it's my issues with my ex-wife I want to send information to the judge but if I print it out its lots of pages so I figure I can send it in a USB flash drive

CyberStrike - June 26, 2019, 1:25 am

(Jun 25, 2019 06:47 PM)bigtoymario Wrote: [\[CITE\]](#) It has nothing to do with kids or terrorism it's my issues with my ex-wife I want to send information to the judge but if I print it out its lots of pages so I figure I can send it in a USB flash drive

Well I have one of those (Ex-wife) so I get it, but also you want to have it documented especially if this is going to court. Look an affidavit is the way to go. Basically with USBs at least on Windows there are artifacts of each USB drive, it's unique. Now you can use a live media (USB/DVD running Linux) there is an application call MAT (Metadata Anonymizing Tool) or ExifTool. Now a days for high value targets the way one writes is analyzed. Yet once again I should really encourage you to do the right thing and do it through the legal process, that evidence would help you in the long run as now a judge will actually consider and weight it.

Jacque Fresco - June 26, 2019, 4:52 am

(Jun 26, 2019 01:25 AM)CyberStrike Wrote: [\[CITE\]](#) Well I have one of those (Ex-wife) so I get it, but also you want to have it documented especially if this is going to court. Look an affidavit is the way to go. Basically with USBs at least on Windows there are artifacts of each USB drive, it's unique.

Now you can use a live media (USB/DVD running Linux) there is an application call MAT (Metadata Anonymizing Tool) or ExifTool. Now a days for high value targets the way one writes is analyzed. Yet once again I should really encourage you to do the right thing and do it through the legal process, that evidence would help you in the long run as now a judge will actually consider and weight it.

Interesting read. I wonder where these Artifacts are actually stored / can be found. However on a freshly wiped USB i just plugged in i noticed several files being created by my machine (System Volume Information\IndexerVolumeGuid & \WPSettings.dat). I wonder whats that (well no longer) and how that what @OP wrote can actually being done. I think reinstalling the OS while the whole drive got wiped in forehand would fix his problems with the artifacts

CyberStrike - June 26, 2019, 6:40 am

(Jun 26, 2019 04:52 AM)Jacque Fresco Wrote: [\[CITE\]](#) Interesting read. I wonder where these Artifacts are actually stored / can be found. However on a freshly wiped USB i just plugged in i noticed several files being created by my machine (System Volume Information\IndexerVolumeGuid & \WPSettings.dat). I wonder whats that (well no longer) and how that what @OP wrote can actually being done. I think reinstalling the OS while the whole drive got wiped in forehand would fix his problems with the artifacts

Thank you for verifying I tend to approach things from a forensic point of view, you would probably have to wipe a few times and overwrite the bits in order to really deal with an investigator finding unallocated space, and either fully or partially recovering the files.

Jacque Fresco - June 26, 2019, 7:06 am

(Jun 26, 2019 06:40 AM)CyberStrike Wrote: [\[CITE\]](#) Thank you for verifying I tend to approach things from a forensic point of view, you would probably have to wipe a few times and overwrite the bits in order to really deal with an investigator finding unallocated space, and either fully or partially recovering the files.

I used <http://www.diskwipe.org/> in the past for this. Its basically Wiping the Partitions. I think its very unlikely that even after just formatting (with zeros) the HDD the found unallocated space would reveal any artifact saying which usb got plugged in. Its like winning the lottery in my mind, but thats absolutly not my special field. But i understand why its a go to for Analyst's

I think what would work too is encrypting the drive with like [VeraCrypt](#), so that Analyst's would need the password. Atleast i read alot that VeraCrypt is one of the best Encryption tools what so ever when you try to hide and encrypt data.