

Forum:[Hack Forums](#)

Thread: [\[TUT\] Windows 7 Anti Forensics. Destroy evidence before it's ever there.](#)

zombiesloth - January 9, 2015, 7:47 am

Warning

I assume if you are on here you are at least smart enough to google if something screws up. Don't send me a message about your fragged drive if you weren't smart enough to use partition editing software or if you skipped rescue disk creation. Plan contingency. An extra usb drive with backups for both FVE, passwords, and other crypto things should be made. Plan paranoid. Scrutinize this system and check the programs yourself. Some fucker posting on HF is not justification enough to believe they are right. If I'm wrong on something, tell me. We can fix this and build a better system for all of us.

Foreword

This isn't pretty since I'm not too good with form posts, but I hope those who read this care about info, not GFX.

This system is for Windows 7 64bit using disks not SSD. I also built this based on current US law on search and seizure. I don't use XP or Vista, so if anyone has AF recommendations/adaptations for them, throw them in the comments to help out others. kk thnx.

Definitions

Definitions

Required: Needed to secure the system.

Optional: Software not absolutely needed but useful for either enhancing security, experience, or anti forensics.

Contamination: The association of critical information with other information, through read, write, file name, file contents. Through attributes such as file time created, accessed, modified. Through histograms, such as access at a time of a certain events in the world. Through social norms/common knowledge, things that an average person would assume would be suspicious or wrong.

Critical information: Information that only targeted individuals should know. This information is able to be stored on disk in a way that can be protected.

Requirements

Required Hardware

Processor capable of handling crypto operations and normal operations.

At least one hard drive for Windows and Storage

One hard drive or media for freedom fighting/critical information

At least one usb drive for keyfiles, password, and other important cryptographic/identifying things

Required Software

Bleachbit

<http://bleachbit.sourceforge.net/>

Truecrypt, or your preference of drive encryption software.

<https://www.grc.com/misc/truecrypt/truecrypt.htm>

Avira, or antivirus of your preference.

<https://www.avira.com/en/downloads>

EMET

<http://www.microsoft.com/en-us/download/details.aspx?id=43714>

Sysinternals suite

<http://technet.microsoft.com/en-us/sysinternals/bb842062>

9Puzzles AF scripts

<https://hackforums.net/showthread.php?tid=3670622>

<http://www3.zippyshare.com/v/31319367/file.html> (password = puzzle9hf)

Required knowledge

Understanding of your jurisdiction's crypto, SnS, investigation laws, and obstruction laws.

Required Browser

Firefox, or a browser of your choice with security hardening support

Tor, either browser bundle or expert bundle depending on your Tor proficiency

Required Browser plugins

HTTPS Everywhere (EFF made)

Noscript

Optional

Optional

Deepfreeze

DBAN

Privacy Badger (EFF made)

Entertainment

Drive Preparation

Drive Preparation

First, we need to prep the drive. This will involve backing up, partitioning, formatting, and finally installation of windows 7.

Backup

This should be obvious. Backup to a disk where there will be as little contamination as possible. Anything critical for freedom fighting should preferably be stored to media in your possession at the time preferably disk. Cloud can be used but encrypt anything you wouldn't want to end up in court beforehand.

Partitioning

Set the partitions in a manner that is useful for you. I recommend a partition for just windows and non disk intensive utilities like web browser and such. Then the second disk be dedicated to games/disk intensive stuff like videos. This will help with disk overhead but you can always drop the second disk for game stuff and put the games in the backup partition. Then a second partition for backup or things that take time to install/re-acquire such as games, utilities like Visual Studio, hi-def dog porn. Freedom fighting, critical information, warez, and high value files should be on a completely segregated disk/media than your current one for windows and non disk intensive stuffs.

Nuking

There are three methods of going about this. In higher to lower security.

Crypto

Encrypt the drive! You can encrypt the system partition of your current windows install and then frag it.

Dban

Boot into Dban and nuke the drive with one of the low pass settings.

Bleachbit

Wipe your free space and recycle bin stuff, while booted in the soon to be nuked Windows installation.

How file systems hold data

How your stuff is stored in Windows

The standard file system for Windows is NTFS. NTFS is a file system supports a Master Boot Record, scalability between 1kb and 64kb for clusters, journaling and other stuff most people don't understand/care. Data can reside on disk but after one pass on a disk above 20 gigs is good because the metal area on the disk (sector) is so close to the next area that it will be very hard to use a magnetic whatever to pull it off. Wipe three times like NSA says and you're cool, but once is enough. Journals log all "transactions" on the disk, reads of files, writes of files, copies, file names etc. 64 meg of "journal" logs.

Installation of Windows

Bootting

Toss in your Windows 7 CD or USB. Next you should be able to see the drives and partitions. Just select your specified partition, measure twice and cut once here. I've screwed up and had to go back several times or have lost data because I had several drives and multiple partitions displayed and I clicked the wrong one and formatted it. Bad move on my part. So measure twice, cut once.

Starting windows for the first time

First, you will want to install all updates except KB971033. That one is optional, just hide it. If you yar-har'd your copy of windows then you definitely don't need it. It's the update that alerts to pirated versions. Even if you didn't, it calls home to Microsoft, takes up space on your drive, and takes up ram just by running. So don't download it. You do however want every other update in the priority download list. Security speaking, you don't want to get popped as you go online. This might be an over night thing depending on your connection. If it is, plan this around bed time and let it go. As of January 2015 there are more than 100 priority updates. This also writes to the disk FLOODING the MFT and any slack space on the earlier sectors of the disk. Now you have plausible deniability since you've downloaded all of these updates. It doesn't say fuck you or have 0's written to the disk, which works out great if you were to be raided by the feds tomorrow. Install the updates and then restart. Install any more, restart, and then get to an area where you can be afk for a while. Now we need to wipe. Using BB, set up to wipe disk space afterwards. Run it and walk away. This might take some serious time. Once this is completed, we will now defrag. Defragging is a plausibly deniable way of moving data around on the disk. Set up defrag on windows and let it defragment the drive or download defraggler from Piriform. After the defrag is complete, you're ready to move on to the next step.

Getting rid of evidence before it's evidence

I like using the automated anti forensics scripts from 9puzzles. I've checked the source, nothing looks out of place on the registry keys and the scripts. If you don't trust the psexec included then you can download psexec from the ps tools list. We will also add a few things that even if our steps do not work, we still have some other protections. It's part of what armies call a "layered defense".

Should something of this not work or be bypassed we have other parts of the defense that might save our ass. We will then add extra features to windows itself not covered before in any other AF tut.

Step one

Run 9puzzle's anti forensics scripts. We need to check to see if everything has worked. We need to check things like last access and USBSTOR.

User assist

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\

If you want, just delete the fucking thing. It's quite simple. Even if it has nolog and what not, just delete the UserAssist key.

<https://gyazo.com/7fcc11446a1631a3050cbfcc08f956e4>

User assist

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR

This should be missing, if its gone, good.

If both of those are set up then that means the scripts ran right. We will not be logged as easily. We still need to disable a few things. This is to be ran in CMD. Search for it, and run as administrator.

Disable the MSCONFIG service

sc config srsservice start= disabled

This needs to be ran because it's going to disable the service.

Disable last access in CMD

fsutil behavior set disablelastaccess 1

Just making sure disable last access is, well, disabled.

Encrypting the page file

fsutil behavior set EncryptPagingFile 1

Now, we need to ensure the page file is encrypted. Why? What happens if you're computer is taken from you? What happens if you're forced to decrypt the drive, the paging file is encrypted with a per boot key. If something is stored there like a key for Truecrypt, then yay, you have at least one more layer of security. Maybe you have something incriminating in there. It's one more level of security. If there is anything, you want to do, it's to get out of that jail cell as fast as possible. 24 hours and they're pressing you for crypto keys, great. Get your lawyer to push for due process. Yay, you're out and you still have layers of security in case you are fucked.

Turing hibernate off

powercfg.exe /hibernate off

Why? You don't want your computer hibernating instead of locking up. Firewire is a serious threat.

Deleting the journal on C:

fsutil usn deletejournal /d c:

The journal is the disk transaction file created by NTFS. This holds 64 megs at least of logs. Any file named on the disk, moved, copied, any deletes, and any transaction. That's a real fucking safety hazard. Why? If you have something named irc.log is written to disk and if you deleted, cool. Until the journal says irc.log was at one point written on the disk. That's bad because if that is a target of the deletion and also a target of an investigation... yeah. Have fun with that anticipatory obstruction of justice charge. Cut the journal every once in a while, wipe, defrag. Simple.

Step Two

Truecrypt time

Truecrypt is still secure. Truecrypt still works. Truecrypt is still a great way to secure your stuff. It's simple, it's still useable. It still has support for the next 5 years at least for Windows 7.

Truecrypt sidenotes

128 AES is the standard cryptographic service for governments... great. Except it doesn't matter who uses it. Look up sigsally and sigaba. Look up DES. NSA has been known to take the most secure keys for themselves even if it's a flawed cryptographic algorithm/machine. AES may or may not be secure, so we just have to assume it's not. The password is hashed 1000 times over to slow down (slightly) brute force attacks or something. I implore you to look into the headers of the Truecrypt volumes. The Truecrypt headers are different for passwords and for keyfiles, not to mention "hidden volumes" aren't that "hidden". Passwords vs Keyfiles. While a password is harder to remember, it is a product of the mind. Great, can't be compelled without a forgone conclusion. Keyfiles have a little bit of an issue with the IV, but other than that could be anything. Good for entropy, bad for security. This means all someone has to do is take all the files off disk, use EnScript and brute force the volumes with the files at hand. The prosecutor can call on forensics to point this out, so you are forced to hand it over. (Passwords are products of the mind, not keyfiles) You can be hit with a wrench until you tell them it's the picture of the cat on your usb drive. Instead you could just make a nonstandard password. Maybe you have a "keyfile" and you can copy a line out of it, type "!@# \$" at the end. Looks like a password in the header. This would give you another method of plausible deniability that you do not know the password. True, you don't know the real password, but you know how to access it. A technicality, but still possible.

Installing new programs and security hardening

Firefox

Now you may have installed firefox already, you may have not. If it's not, download it. Sure it may have the most disclosed vulnerabilities, but that's one less hole hoarded in an "contractor's" Oday usb drive.

HTTPS Everywhere

<https://www.eff.org/https-everywhere>

Download it from EFF's website. Don't use the observatory. While this may seem like a bad idea, let's look at it. Firstly, using observatory is more overhead. Secondly it's identifying. Thirdly it isn't anonymized unless you have expert bundle.

Mailvelope

<https://www.mailvelope.com/>

This is an optional that I didn't list up top because I really don't like the idea of doing crypto on a dirty machine, let alone comms on a dirty machine, even worse lull you into thinking that a SQL db with keys in your browser which is attackable is a great idea.

NoScript

<https://noscript.net/>

This is a given. Use it. It may be annoying to unlock certain sites and keep tracking off, it's better in the long run. Security is always at odds with convenience.

EMET

<http://technet.microsoft.com/en-us/security/jj653751>

<http://www.microsoft.com/en-us/download/details.aspx?id=43714> (5.1)

This is basically a stack watching program. It changes how they work, throws some canaries in, other thing. It can be bypassed. So why install it? Because, most exploits written do not support

EMET bypassing. So you have a chance of saving yourself by having FF run under this. Same with your irc client, same with any other program that touches the internet.

Sysinternals

Sysinternals is a set of programs written by a bad ass named Mark Russinovich. He worked for his own little company. He was then picked up by Microsoft. He now works as a happy code monkey to this day for them. He still makes wonderful tools like process explorer and rootkit revealer. You will want to extract a folder named Sysinternals. Afterwards, move it to "C:\Windows\System32". CMD starts there so if you need to get to lets say, psexec.exe inside there. Or shellrunas.exe. That's why I prefer downloading Sysinternals. Two downloads in one click. Sysinternals is needed because you can string programs easily, check running programs, check the signing keys on programs, protecting yourself from malware.

Step three

ubnt123 - January 9, 2015, 7:59 am

unread able sorry ,maybe when i will have a time,thanks anyway.

zombiesloth - January 9, 2015, 8:06 am

DeepFreeze

Install DeepFreeze, you will want to create a password that you can type in easily and remember. Uninstall the master thingy, this prevents someone coming in and using the one time password thing on your computer. This will help mitigate state sponsored intrusions as well as savvy intruders. The only issue with this is the freespace farther down the disk is used for DeepFreeze's sandboxing capabilities. Also since DeepFreeze is not as often attacked as sandboxing programs like SandBoxie or Comodo's antivirus sandbox. So you are less likely to see exploits for DeepFreeze. Do not take this as a guarantee that you are invulnerable. This is just a part of the layered defense of your machine.

Knowledge finding stuffs

Reading on US Federal interpretations of Search and Seizure, crypto, and obstruction laws.

http://www.wylielaw.com/arrests_stopsearches.html

<http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>

<http://www.njcctf.nj.gov/pdf/cmpmanfi.pdf>

<http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf>

<http://www.forbes.com/sites/andygreenberg/2012/02/24/two-cases-lessons-if-cops-dont-know-what-you-encrypted-they-cant-make-you-decrypt-it/>

https://www.eff.org/files/filenode/us_v_fricosu/fricosuamicus7811.pdf

<http://www.wired.com/2012/01/judge-orders-laptop-decryption/>

<https://www.ohiobar.org/forpublic/resources/lawyoucanuse/pages/lawyoucanuse-132.aspx>

<http://www.perkinscoie.com/images/content/2/4/v2/24154/lit-11-06funkfeaturemay.pdf>

<https://ssd.eff.org/en>

http://en.wikipedia.org/wiki/Daniel_Dantas_%28entrepreneur%29

<http://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/>

http://www.theregister.co.uk/2010/10/06/jail_password_ripa/

<http://www.informationliberation.com/?id=38545>

Videos on US Federal interpretations of Search and Seizure, crypto, and obstruction laws.

<https://www.youtube.com/watch?v=lqBVAcxpwio>

<https://www.youtube.com/watch?v=Jt7D4AlfqIQ>

<https://www.youtube.com/watch?v=ibQGWXfWc7c>

What happens when you piss off the feds.

<http://watchdog.org/110099/data-privacy-snooping-claims-mount-against-mn-cops-government-employees/>
<http://www.wilderssecurity.com/threads/suspect-ordered-to-decrypt-his-own-data.347853>
http://www.wired.com/images_blogs/threatlevel/2013/04/fedswantdecryption.pdf
<http://www.law.cornell.edu/supct/html/96-1469.ZS.html>

EXTRAS

Winrar

Settings in Winrar allow you to set it to wipe after encrypted or all compressed packages are closed. Set it for all. This will wipe any of the /temp/ stuff made by winrar.

<https://gyazo.com/ff64129abb442cf701bd6600160e95c3>

Adobe Reader

HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\10.0\AVGeneral\cRecentFiles
Start Regedit.exe with administrative rights. Go to the key above. Delete it. Become winrar.

Bleachbit

To add extra functionality to bleachbit, please check in settings "overwrite files" and "Download and update cleaners from community".

<https://gyazo.com/88f530800f7cdc407f729c69dc5df479>

zombiesloth - January 30, 2015, 3:29 am

Truecrypt Extras

So Truecrypt is a pretty useful tool and much of the security of this plan hinges on the use of Truecrypt. Using it properly is very important. We need to have both passive and active anti forensics techniques.

Preferences

So we're going to want to set a few things in place, either click all the stuff I have set or read along and learn while doing it.

<https://gyazo.com/ecf6e31f8e4c84ae6d19e8a8511746b6>

Default Mount Options

Mount volumes as read only is quite useful if you just read from the section. Maybe a collection of E-books or something or pictures. But if you want to add you will have to make sure you mount as read and write. Mount volumes as removable media is an option to make it look like usb connections or something. The mac is still the same as your drives. But if the government executes a search warrant and checks your drive and somehow determines through undeleted logs that it is the drive you're SOL. Personally I don't set the drives as read only and mount as removable media because they serve no use to me since I read and write a lot to my encrypted disks.

Truecrypt background task

Enabled just means that it goes to a background task. (out of sight but still works) Exit when there are no mounted drives does exactly how it sounds. I never know when I need/want to mount the drives so I keep that off.

Actions to perform upon logon to Windows

Start Truecrypt as a background task is a default option. It starts it and its ready to go on boot.

Mounting all devices is a bad idea because you could have a cached keyfile or password and could potentially auto mount after logging in. Go with the defaults on this one.

Auto Dismounts

This is where the good stuff happens. User logs off. Obvious. Make sure its locked. 5 minute lock screen + this = no asshole steals your stuff when you are logged off (Even if they have a root shell on your box). Entering power saving mode shouldn't be enabled because if you're a laptop user then this is a bad idea. Especially if you're at 10% battery and you have a drive you're trying to work on. Auto dismount after 60 minutes of no read/write. If you're not using it then why the hell is it logged in? Force dismount is important if the drive needs to disconnect for some reason. Good for security, bad for convenience.

Windows

Open explorer... obvious. Its pretty useful because I hit enter after mounting and causing it to dismount. Taskbar? Basically yellow vs blue like to know if something is connected or not? Don't change it. Preserve modification timestamp. We need to change this. Do you want to preserve modification times? No. This is good data for the forensics teams pouring over your box.

Password Cache

Caching the passwords is a bad idea. That stores it in memory. Either page file or ram. Either way a bad idea. Wipe Cached passwords on exit. In case it somehow gets cached we want to wipe it. Wipe cached passwords on auto-dismount. This is a backup incase it gets auto dismounted and there is a cached password/keyfile.

Auto Dismounts

This is where the good stuff happens. User logs off. Obvious. Make sure its locked. 5 minute lock screen + this = no asshole steals your stuff when you are logged off (Even if they have a root shell on your box). Entering power saving mode shouldn't be enabled because if you're a laptop user then this is a bad idea. Especially if you're at 10% battery and you have a drive you're trying to work on.

Truecrypt Keybinds

This is probably one of your last lines of defence. If you get Barrett Brown'd, you can atleast hit Ctrl-Alt-S or something and boom. Make sure it's dismount all, forced, and wipe cache. This is one of the last sure fire ways to drop all drives quickly.

<https://gyazo.com/202e6eb1b28bbe3e48bd5676b8a8ef25>

Pazician - January 30, 2015, 4:11 am

Nice tutorial man, I'm happy to see someone post a tutorial based around Anti-Forensics as it's a pretty serious topic. Cheers to you!?

zombiesloth - January 30, 2015, 6:11 am

(Jan 30, 2015 05:11 AM)Pazician Wrote: [\[CITE\]](#) Nice tutorial man, I'm happy to see someone post a tutorial based around Anti-Forensics as it's a pretty serious topic. Cheers to you!?

Thanks, I was kinda getting tired looking around for stuff on real AFT. Plus people just say "run this" or "do this" without much reason behind it. I try to back my stuff up with OSINT and publicly known forensics techniques. If you build a machine like it's compromised from day one then you know each potential threat and you hopefully have a counter measure to each REASONABLE threat.

zombiesloth - April 6, 2015, 7:05 pm

Commsec

Commsec in military parlance is Communication Security. Secure communications channels are hard to come by these days. And those that are have a lot of finger prints or are complex to use. So what do?

Scenario

So lets assume we have an insecure channel (internet, lan, wan) where you and the other party are trying to transfer data. You assume worst case, an active attacker has MITM capabilities and has the ability to capture all comms (voip, ftp, ssh, tcpip) and store for later mining/analysis.

File transfer

Lets say you have a nice ol' CSV at around 100mb. But you want to send it to your friend in IRC. You're going to need WinRar or another equivalent tool with the ability to compress and encrypt. NSA recommends SecureZip and WinZip, but I prefer WinRar because it's what I've grown up on and its pretty a pretty common install. You're going to need to select the file you wish to compress and set it for whatever compression detail you like. Both of you will need to know the password, I will go into this later.

Split Code Generation

So you read the first paragraph and maybe said something to the tune of 'how do I make transmit these passwords' or 'how do you share a secret like these?' And there are a few ways.

[color=#FF0000]Channels for Sending split keys.

Firstly we need to know how to send it. We have many channels to send stuff in. XMPP, skype, irc privmsg, email, text messages, phone calls, or even pictures in a 4ch thread. You need to have have several different ways of sending parts of the shared secret and signalling which part of the split it is. I personally like Sending half of it in xmpp and sending a privnote link for the second part. This ensures they get both parts securely and that I can see the target got the privnote part.

How 2 N2 Split Keys

There are a few ways to generate these. There are alphabet based and numeric based. I've yet to make one that works reasonably with alpha numeric besides adding two of these together which takes too long in my opinion.

Chain Addition

This shit is dead simple, it's a basic Linear Feedback Shift Register (a crap "random" number generator that in principal many of your PRNG's work on) and it's so easy a caveman can do it. Lets take the phrase ZombieSloth and make it into a seed for this.

Firstly we need to split it into 10 letter groups.

ZOMBIESLOT | HZOMBIESLO

and now we number the letters off in alphabetical order

ZOMBIE SLOT | HZOMBIESLO

06 5132 8479 30 76142958

add the two parts together with modulo 10

06513 28479

30761 42958

36274 60327

Voip

<https://gyazo.com/3a8b240c4d1b960c695a62094cc6c546>

As you read this transcript of a call I want you to try to make an educated guess on what they're talking about. What are the two individuals talking about. Anyone can see they are talking about papers on a table. But if you rub two of your brain cells together, then you might see they are talking about a drop and time. But what if I told you this is a talk between an American spy and the

SVR(Russian Intelligence). Now what if I told you this was the talk to tell Robert Hanssen why the drop was screwed up under a bridge. Use of ambiguous talk code words can stall or confuse adversarial forces. The Paris shooters used code words and burners. The code phrase for the start of operations for the 9/11 hijackers and planners used code phrases like "The refrigerator will be delivered." and others to foil eaves droppers. The reason codes work is because without context you can only find out what a code means after the event.

https://www.nsa.gov/ia/_files/factsheets/I735-002-08.pdf

https://www.nsa.gov/ia/_files/factsheets/Encrypting_Files_with_SecureZIP.pdf

decko22 - April 9, 2015, 2:05 am

This is awesome post,thank you so much for more information..thanks

zombiesloth - May 23, 2015, 6:07 am

Why do split keys and codes matter?

Well, think of it like this. All you have to do is go into a compromised IRC and have an innocuous conversation to tell them the zip/rar password if you're using symmetric encryption. Some of the tools out there support asymmetric, but file size constraints may be preventing you from doing asymmetric. There is a chance the stool pigeons (ha cha cha cha) won't know the password or a passive/active adversary (feds) might think nothing of the conversation. This allows some communications security because those in the know can derive the password/meaning from the conversation.

You and your friend must be able to work the code words into the conversation and hint at the words as being code words. A way to secure this would be to use the half sent with the file and the other half conveyed to the person you are trying to trade with.

ZOMBIESLOT/H is the first half (possibly transmitted in a conversation :3)

065 1328479
616 4502165
770 9523712
479 4750836

HACKFORUMS as the second half (possibly sent as the file name or source of the leak/db/whatever)

412 53780 69
537 80586 54
805 85341 92
853 38750 10

You can do this with both words larger and smaller than 10 characters. They can either be chopped down to 10 characters or can be repeated to the nearest 10th. Whichever floats your little pixel boat and your friends.

ORGANOPHOS/PHATEORGAN
592 1468 370/851 0379 426

So if we received the code word zombiesloth and we have a file named hackforums.csv, you could generate the password for the file. Both examples are listed above. You take those digits and add them together to get the final password for the file. Do note you are using mod 10, so there is no carry of digits when you get 11,12,13 etc as your sum. In those cases you would have gotten 1,2,3.

Warning, if you use the first 10 digits of the PRNG stream generated your results will be FAR less

than random. In fact, 3.6 million possibilities for the first 10 digits. Not very... suitable for our purposes.

61645 02165 77095 23712 47947 50836 PRNG Stream Zombiesloth
53780 58654 80585 34192 85338 75010 PRNG Stream Hackforums
14325 50719 57570 57804 22275 25846 Key (Digit wise addition mod 10)

Finally you can paste that into the password field and get access to your mad Oday stockpile. You would go through the same steps to both make the password/set it as you would to decrypt it, so it becomes obvious who can't do addition in your group when passwords are "messed up". I wouldn't use this PRNG for anything NSA standard but I would definitely use this to protect a few zips holding stuff on FTP servers.

zombiesloth - May 25, 2015, 9:33 pm

A side note on deleting files

If you do not need a file (Logs, pictures, that episode of MLP) just delete it permanently. You can do that, just make sure you use SHRED FREE SPACE in Bleach Bit. This is very similar to the "shred file" that is now added when you right click. I prefer doing this because I don't have to go through the monotony of shredding each file or moving everything to a folder to delete it in one swoop.

Step one

Select Bleach Bit to wipe free space. This wipes all unallocated spaces on the drive. (including "permanently deleted" windows files)

Step two

Select the drive, you want to make sure its the drive you want to delete on. Don't do this if you have a "hidden operating system".

Step three

Take a coffee break, smoke break, etc. This will take some time depending on drive size. The little file at the bottom is where Bleach Bit makes a file and just writes random data to it.

This is doing the "shred" on your whole drive where there is no allocated data, meaning you deleted that tentacle pic, it will wipe it over. Just run this over night or after you've cleaned and defragged to make sure everything is squeaky clean.

e-Whoring Legend - July 11, 2015, 6:57 pm

Damn man this tutorial is so fucking detailed. Thanks a lot for the dedication to the thread.

NegativeGamer - July 12, 2015, 6:22 pm

wow thank you bro tutorial really helped me!

DarkTruTH007 - July 16, 2015, 7:10 am

nice and informative post.....

OG-SB - July 16, 2015, 7:16 am

thanks for this i will see soon

arnographic - July 18, 2015, 7:47 am

this guide definitely will help me out ! thank you for this sharee

zombiesloth - July 19, 2015, 2:48 am

There's some more stuff I can put in here and do, I should probably remake the whole thread and do some YT tuts because this shit looks hella over complicated when I look at it now.

Evil Corp - July 19, 2015, 9:56 pm

Let me know once you update this OP.

ccxxvr - July 20, 2015, 6:39 pm

Interesting read, thanks for details.

Aurora - July 20, 2015, 11:02 pm

(Jul 19, 2015 02:48 AM)zombiesloth Wrote: [\[CITE\]](#) There's some more stuff I can put in here and do, I should probably remake the whole thread and do some YT tuts because this shit looks hella over complicated when I look at it now.

YouTube tutorials would be definitely nice.

gausho - July 21, 2015, 10:58 am

amazing tutorial. thank you very much for this

zombiesloth - July 25, 2015, 10:18 am

I'm just record a bunch of segments, throw it into whatever video editing stuff I have and put it up on the interbutts. I'm recording now, dunno if my lamer brother will say something stupid while I'm doing this. cri cri D:

magos - July 31, 2015, 5:06 am

Very nice! Thank you man :)

mr_boss - August 3, 2015, 11:38 am

This tut is so fucking HQ and detailed!
wow , thanks man ?

KnockSteadys - August 19, 2015, 10:20 pm

very nice well explained tut man

zombiesloth - December 8, 2015, 12:24 pm

New thread on this maybe in a month if I stop being lazy. I'll show a way faster way of doing this.

shabahighrank - December 6, 2016, 2:27 am

nice tut, thank you for the share

phpmaster1 - December 6, 2016, 4:42 am

Good read bro, very nice share xD