

Forum: [Hack Forums](#)

Thread: [Covering Your Tracks](#)

LK) - January 11, 2012, 11:23 am

[IMG]<http://img600.imageshack.us/img600/1035/bourned.png>[/IMG] 1) VPN

Russian Server – IP Address

<http://nvpn.net/>

2) Tor Tunnel

No individual relay ever knows the complete path that a data packet has taken.

www.torproject.org

3) A busy Public Wifi

use a disguise and use cash only

Or

3a) Use long range wireless adapter

Several Blocks away

2000mW 2W 802.11 G / N High-Gain USB Wireless Long-Rang WiFi Network Adapter 9dBi Rubber Antenna

WEP is still used and easy to crack

WPA/WPA2 is cracked with Reaver and will recover the target AP's plain text passphrase in 4-10 hours (linux only)

[IMG]<http://imageshack.us/a/img842/8572/alfap.png>[/IMG]

4) Spoof Your Mac Address

<http://www.technitium.com/>

5) Encrypt Hard Drive or keep your hard drive wiped so that no information exists on your computer

When traveling through borders its better have a clean system than an encrypted drive because known hackers get searched

www.steganos.com

Many Linux distros have full disk encryption

6) The Amnesic Incognito Live System (TAILS)

Tails is configured with a special care to not use the computer's hard-disks, even if there is some swap space on it. The only storage space used by Tails is the RAM memory, which is automatically erased when the computer shuts down. So you won't leave any trace neither of the Tails system nor of what you did on the computer.

<https://tails.boum.org/>

Also use for a more secure messaging:

<https://crypto.cat/>

7) Cell phones can determine your location even when off.

Either take the battery out of your cell or place in a different location.

Smart phone pictures have geo tags and can determine your location

In addition to carrierIQ collects info

<http://arstechnica.com/apple/news/2011/04/how-apple-tracks-your-location-without-your-consent-and-why-it-matters.ars>

8) Use <https://startpage.com> no logs

Google keeps logs and your searches can be used against you.

<http://donttrack.us/>

"The U.S. government asked Google for data on its users more than 31,000 times in 2012 alone, for example. And the government rarely obtained a search warrant first, Google recently revealed; in nearly all cases, the company ended up turning over at least some data."

Additional Notes:

Evidence that can be taken in a warrant: Plan as though you were going to be raided

[IMG]<http://imageshack.us/a/img685/9518/searchrj.png>[IMG]

Never have anti forensics tools on your computer or on digital media ex. CD, DVD, USB in plain sight.

Investigators have to establish a link between the IP address, computer and the person causing the activity. These steps minimise that link.

Absolutely never user your real IP and physical address.

"the Rapid Information Overlay Technology (Riot) software uses photographs on social networks. These images sometimes contain latitude and longitude details – automatically embedded by smartphones within so-called 'header data'. Riot pulls out this information, analysing not only the photographs posted by individuals, but also the location where these images were taken" source from <http://www.guardian.co.uk/>

[IMG]<http://img9.imageshack.us/img9/8208/locqc.png>[IMG]

Microsoft seeks patent for spy tech on

[IMG]<http://img541.imageshack.us/img541/8168/13702359.png>[IMG] Most likely they are already doing this.

[IMG]<http://imageshack.us/a/img27/4880/skypeusq.th.jpg>[IMG]

'Legal Intercept' would allow it to silently record VoIP communications.

US gov't has a Internet scouring program, code-named PRISM, that records Internet activities: Lots of internet traffic from the west passes through the US because the destination servers are there, or connect there. Encrypting email using PGP is one possibility, though it is not easy to set up. Systems such as Tor, together with a virtual private network (VPN) connection, can cloak your location, though your identity might still be inferred from the sites you connect to.

[IMG]<http://img197.imageshack.us/img197/2458/oqw9.jpg>[IMG]

www.guardian.co.uk

If you done everything correctly: Microsoft Watched but couldn't catch a hacker.

"Va.-based computer security firm Global Integrity, said Microsoft's failure to catch the hacker is not surprising."

<http://abcnews.go.com/Technology/story?id=119324&page=1>

[IMG]<http://imageshack.us/a/img607/3086/catchw.jpg>[IMG]

[Video: <https://www.youtube.com/watch?v=i8z7NC5sgik>]

The US Supreme Court has held that "a witness may have a reasonable fear of prosecution and yet be innocent of any wrongdoing. The privilege serves to protect the innocent who otherwise might be

ensnared by ambiguous circumstances."

"...any lawyer worth his salt will tell the suspect in no uncertain terms to make no statement to the police under any circumstances."

R.I.P. Aaron H. Swartz (November 8, 1986 – January 11, 2013)

[IMG]<http://imageshack.us/a/img585/6549/aaronswartz791n.jpg>[/IMG]

prasad - February 11, 2012, 12:39 pm

Hii..valuable info bro.. keep going..

triqih - February 11, 2012, 1:04 pm

thx bro just what I needed ?

this will help me alot

xswrain - February 11, 2012, 1:33 pm

6) The Amnesic Incognito Live System (TAILS)

Wouldn't the removal of swap space dramatically reduce the amount of memory that can be used?

Romanov - December 20, 2012, 1:38 am

helpful...nice...tnx for this very much m8:)

LK) - February 13, 2013, 8:37 am

I have updated some of the information.

4RG0S - February 13, 2013, 2:18 pm

This is a great Thread and also great Info, but i think it is too late now. What can i do ? :)

Jay? - February 13, 2013, 2:27 pm

(Feb 13, 2013 03:18 PM)4RG0S Wrote: [\[CITE\]](#) This is a great Thread and also great Info, but i think it is too late now. What can i do ? :)

Smash your HDD and hope for the best?

Di?mond - February 13, 2013, 2:45 pm

Glad this was posted this will help people when wanting to be anonymous when doing something.

trinkkits - February 13, 2013, 5:03 pm

This is awesome. Thank you for sharing :)

LK) - February 13, 2013, 6:44 pm

(Feb 13, 2013 03:18 PM)4RG0S Wrote: [\[CITE\]](#) This is a great Thread and also great Info, but i think it is too late now. What can i do ? :)That would be part 2. "How to protect yourself if your in panic mode"

Isidar - February 16, 2013, 2:13 am

LK) is an awesome member!

Good luck with getting awesome reviews as this is an awesome tutorial.

DaFreak - February 16, 2013, 3:53 am

Great information.. Thanks for Cryptocat ;)

LK - February 16, 2013, 5:15 am

(Feb 16, 2013 04:53 AM)DaFreak Wrote: [\[CITE\]](#) Great information.. Thanks for Cryptocat ;)Skype you can sniff the user's IP and also with the skype resolver. (without the patch if it works).

SIM-1589588 - February 16, 2013, 5:22 am

(Feb 13, 2013 03:27 PM)Remorse Wrote: [\[CITE\]](#) Smash your HDD and hope for the best?
Or just drop it into sea....

@LK Nice guide mate :)

LK - February 16, 2013, 6:37 am

(Feb 13, 2013 03:27 PM)Remorse Wrote: [\[CITE\]](#) Smash your HDD and hope for the best?
Hardware based forensics is very good compared to software forensics, so you would have to completely destroy your hard drive, so that there is nothing left but ashes.

???? - February 25, 2013, 6:34 am

Thanks for sharing it with us Man :)

Fluoxetine - February 25, 2013, 6:52 am

(Feb 16, 2013 06:22 AM)???????????????????? EMS Wrote: [\[CITE\]](#) Or just drop it into sea....

@LK Nice guide mate :)
or put it in a microwave and run lol

LK - February 25, 2013, 7:49 am

(Feb 25, 2013 07:52 AM)Fluoxetine Wrote: [\[CITE\]](#) or put it in a microwave and run lolDon't use defrost because it's not as strong.

zwatcher - February 25, 2013, 6:21 pm

Thanks for contributing dude , you trying to help the community that's admirable

z'watcher

LK - February 25, 2013, 7:08 pm

(Feb 25, 2013 07:21 PM)zwatcher Wrote: [\[CITE\]](#) Thanks for contributing dude , you trying to help the community that's admirable

z'watcherEverything we do leaves a trail somewhere.

Acroz - February 25, 2013, 7:25 pm

This is a GREAT tutorial for anyone who doesn't know how to protect themselves and stay anonymous!

GREAT topic!

LK - February 25, 2013, 8:16 pm

(Feb 25, 2013 08:25 PM)Se7enX Wrote: [\[CITE\]](#) This is a GREAT tutorial for anyone who doesn't know how to protect themselves and stay anonymous!

GREAT topic!Thanks and some of those things were not aware of.

?Blackeye™ - March 2, 2013, 5:31 am

Thanks bro for all this informations. that's just awesome.

LK) - March 2, 2013, 8:57 am

Something to consider before you test your skills.

NewOnStreets - March 2, 2013, 9:24 am

Awesome guide. All information in one place. Will be helpful for sure ;)

LK) - March 2, 2013, 9:26 am

(Mar 2, 2013 10:24 AM)NewOnStreets Wrote: [\[CITE\]](#) Awesome guide. All information in one place. Will be helpful for sure ;)Wow, your first post to the forum. Thanks

NewOnStreets - March 2, 2013, 9:30 am

Just looking around.. And it's not hard to stop and say Thanks for useful information :)

Keystrokes - March 2, 2013, 9:45 am

thanks for sharing this. very useful

einbrettholz - March 2, 2013, 10:14 am

<https://crypto.cat/> is owned by the feds.

didnt you read the leak?

i think it hillarious :)

LK) - March 2, 2013, 10:30 am

(Mar 2, 2013 11:14 AM)einbrettholz Wrote: [\[CITE\]](#) <https://crypto.cat/> is owned by the feds.

didnt you read the leak?

i think it hillarious :)What is your source about crypto.cat?

phlow - March 2, 2013, 10:48 am

(Mar 2, 2013 11:14 AM)einbrettholz Wrote: [\[CITE\]](#) <https://crypto.cat/> is owned by the feds.

didnt you read the leak?

i think it hillarious :)

The owner/project manager/whatever you want to call him is under surveillance by the feds.

This does not mean that CryptoCat is owned by the feds.

einbrettholz - March 2, 2013, 10:52 am

hey lk)

i cant find the leak anymore, weird.

but if i recall correctly that bill binney guy leaked it.

dunno, could also have been cryptome in retrospect.

LK) - March 2, 2013, 1:23 pm

(Mar 2, 2013 11:52 AM)einbrettholz Wrote: [\[CITE\]](#) hey lk)

i cant find the leak anymore, weird.

but if i recall correctly that bill binney guy leaked it.

dunno, could also have been cryptome in retrospect.Obviously, there's a big difference being under surveillance and owned.

Magnum_357 - September 25, 2013, 4:38 am

This is very good and useful information ! Tnx for sharing bro :) ?

Pyromaniac1 - September 25, 2013, 5:06 am

Thanks for the tut, really detailed!

LK) - September 25, 2013, 9:04 am

If there is anything I left out please feel free to comment.

adampelletgun - September 25, 2013, 9:08 am

(Sep 25, 2013 09:04 AM)LK) Wrote: [\[CITE\]](#) If there is anything I left out please feel free to comment.
Maybe add DuckDuckGo and Hotspot Shield?

Nice thread also.

LK) - September 26, 2013, 4:12 am

I had started using duckduckgo before startpage.

Lightsout - September 26, 2013, 7:55 am

So far so good:

Track of what ive done so far :

VPN (English ip)
Tor
Mac Address Spoofer
Crypted my HDD

Waiting:

Public Wifi

-

Hopefully im Invisible :D

Thanks LK!

snorlaxlulz - September 27, 2013, 9:37 pm

So what should i use besides of Google?

LK) - September 29, 2013, 5:21 pm

(Sep 27, 2013 09:37 PM)snorlaxlulz Wrote: [\[CITE\]](#) So what should i use besides of Google?

<https://www.startpage.com>

<https://www.duckduckgo.com>

are some safer alternatives.

laxcats - September 29, 2013, 10:31 pm

Thank you alot now i know more ways to hide myself :D

LK) - September 30, 2013, 11:32 am

(Sep 29, 2013 10:31 PM)laxcats Wrote: [\[CITE\]](#) Thank you alot now i know more ways to hide myself
:DAs many are not aware of the information google collects on its users.

?_f?¢??ff_? - September 30, 2013, 11:47 am

Nice Tut man :D bit hard to follow at some points but really good :D

LK) - September 30, 2013, 11:51 am

(Sep 30, 2013 11:47 AM)?_f?¢???ff_? Wrote: [\[CITE\]](#) Nice Tut man :D bit hard to follow at some points but really good :DWhat points are hard to follow? Thanks

Cyprella - October 15, 2013, 1:07 am

Wow, didn't know all this. I thought Facebook stripped all the EXIF data? I guess it doesn't remove the location data. Thanks, it was a good read!

TuTu - October 21, 2013, 9:17 pm

Thanks a lot, great tutorial! Really useful information.
That lawyer guy in the bottom video is crazy, haha.

Asp1r3-At0m - October 21, 2013, 9:48 pm

Nice thread bro!

also when going AFK, NEVER, for the love of God, NEVER say something about the stuff you do and never tell or give anyone the nick you use :)

I usually when doing some stuff, I love to use a fake name, but I only do this due to some circumstances

EpyonGun - October 21, 2013, 9:52 pm

@OP

- 1: Most vpns WILL cooperate with federal/fraud investigations 9x/10
- 2:<3tor (but still far from untraceable)
- 3: You cannot hide from security cameras this is 2013
- 3a:reaver ONLY works when WPS is ON which businesses almost never do
- 4: any decent router with anti mac spoofing is going to give you a dead connection
- 5: No public HDD encypter is going to hide your porn collection from a 1.3million\$\$ folding pc
- 6: tails is horribly flawed
- 7: see #3.--^
- 8:Chances are if you are already here you have already used google for something that can be used against to in the court of law to have your ass put in jail

Really hope people dont think they are really covering anything by only doing whats listed.
I hardly know anything about computers and know none of this stuff would be any good

Jay? - October 21, 2013, 9:57 pm

A lot of what Epyon said is solid.

Best advice you gave was TOR.

But even though it should be properly set up and secured on a secure box.

Jack Bauer - October 21, 2013, 10:04 pm

(Oct 21, 2013 09:57 PM)Cyb3rCOMpl3x Wrote: [\[CITE\]](#) A lot of what Epyon said is solid.

Best advice you gave was TOR.

But even though it should be properly set up and secured on a secure box.
TOR is kind of risky right now isn't?

NSA, FBI are dragging their balls across the floor on TOR.

Jay? - October 21, 2013, 10:06 pm

(Oct 21, 2013 10:04 PM)Jack Bauer Wrote: [\[CITE\]](#) TOR is kind of risky right now isn't?

NSA, FBI are dragging their balls across the floor on TOR.

<https://hackforums.net/showthread.php?tid=3817861&pid=35853200#pid35853200>

Read that as i cba to retype it.

I33ch3r - October 22, 2013, 11:55 am

Cool tut, too bad I found it too late. Guess I will just destroy my disks when feds arrive :D

Xen0n- - October 22, 2013, 1:27 pm

CyberComplex's correct on his stand with Tor, the Tor network is fine right now.

<https://prism-break.org/> Might wanna check this out others, great site.

Noxite - October 22, 2013, 1:45 pm

Nice job with the thread. Go steps to take into account. Though, the thread design could have been created with some better overview.

bozboz - October 22, 2013, 2:08 pm

thanks for sharing..russian vpn is the best:d

041798 - October 22, 2013, 4:47 pm

Very helpful. Thank you for sharing this

Malfishcake - November 5, 2013, 5:33 pm

Pretty scary how easily our info is spread... Thanks for these methods :)

SIM-1980240 - November 5, 2013, 8:33 pm

(Oct 21, 2013 10:04 PM)Jack Bauer Wrote: [\[CITE\]](#) TOR is kind of risky right now isn't?

NSA, FBI are dragging their balls across the floor on TOR. There have been a lot of misconceptions about TOR lately. The FBI and NSA haven't infiltrated the TOR network. What they have done however is take down freedom hosting, which was the main hosting company for many websites on the deep web. Then use those sites for an firefox exploit that identifies your actual IP address. So as long as you're using TOR for privacy on the surface web. You should be perfectly fine. ?

LK) - January 9, 2014, 3:39 am

Given enough time and resources nothing is absolutely secure but you can certainly put more roadblocks.

AntiHacker - January 22, 2015, 12:06 pm

this is nice thanks so much for sharing mate

LK) - January 22, 2015, 5:59 pm

The more random your methods the better chances you have of staying under the radar.

FluxHax - January 23, 2015, 3:06 am

Awesome, thank you. 5 stars thread.