HOW TO SAFELY SUBMIT COMMUNIQUES TO MTLCOUNTER-INFO.ORG

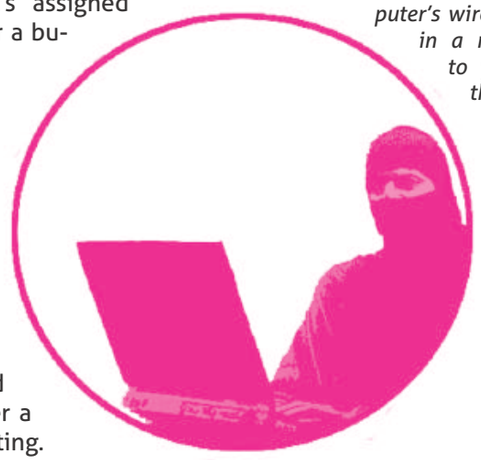
We thought it would be useful to summarize a basic technique to anonymously submit communiques, using the Tails operating system.

Tails is a computer operating system designed with security in mind, which can boot off a USB or CD, from any computer. After shutting down Tails and ejecting the USB or CD, the computer can start again with its usual operating system. Tails is designed to leave no trace on the computer by not interacting with the hard-disk, and only using the RAM for memory (which is automatically erased when Tails shuts down). In addition, it forces every internet connection to go through the ***Tor network***[i], so is much safer than using just a Tor browser on your normal operating system.

IP and MAC addresses:
Every internet connection has a specific ***IP address***[ii] that can be logged by websites that are visited, and which reveals the connection that was used. An IP address can be traced to the internet subscriber it's assigned to, whether an individual or a business like a café.

Every computer has a ***MAC address***[iii] , which can identify the specific computer that connected to a site via the IP address.

Tails automatically conceals the IP address by using the TOR network, and automatically gives the user a fake MAC address upon starting.



i. *TOR is a network of proxies run by volunteers with the explicit purpose of maintaining anonymity online. With TOR, your connection goes through three proxies. You connect to TOR and each of the three proxies (nodes) you access encrypts your data. No individual node can know both what you are connected to and who you are. The third node decrypts the data and accesses the website, sending the information back through the proxies in encrypted form.*

ii. *An Internal Protocol address is a string of numbers that allows you to send and retrieve data over an internet connection (for example, 78.125.1.209). This number identifies the location, Internet service provider, and technical details of your connection. It is comparable to a house's street address. An unobscured IP will lead investigators directly to your connection.*

iii. *The Media Access Controller address specifically identifies your computer. If you access the internet, the router may log your MAC address and maintain that log. If investigators were to read the logs of a router you accessed (say, a public wifi from which a communiqué was sent), and then compare that address with the MAC address of your computer's wireless card (say, confiscated in a raid), you'd be connected to your activity while using that router's connection. If the MAC address is not changed, there is the possibility of your activity being traced back to you if investigators are persistent or lucky enough.*

HOW TO SAFELY SUBMIT COMMUNIQUES TO MTLCOUNTER-INFO.ORG

We thought it would be useful to summarize a basic technique to anonymously submit communiques, using the Tails operating system.

Tails is a computer operating system designed with security in mind, which can boot off a USB or CD, from any computer. After shutting down Tails and ejecting the USB or CD, the computer can start again with its usual operating system. Tails is designed to leave no trace on the computer by not interacting with the hard-disk, and only using the RAM for memory (which is automatically erased when Tails shuts down). In addition, it forces every internet connection to go through the ***Tor network***[i], so is much safer than using just a Tor browser on your normal operating system.

IP and MAC addresses:
Every internet connection has a specific ***IP address***[ii] that can be logged by websites that are visited, and which reveals the connection that was used. An IP address can be traced to the internet subscriber it's assigned to, whether an individual or a business like a café.

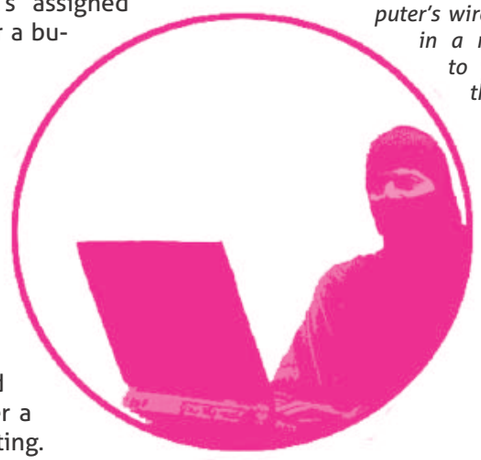
Every computer has a ***MAC address***[iii] , which can identify the specific computer that connected to a site via the IP address.

Tails automatically conceals the IP address by using the TOR network, and automatically gives the user a fake MAC address upon starting.

i. *TOR is a network of proxies run by volunteers with the explicit purpose of maintaining anonymity online. With TOR, your connection goes through three proxies. You connect to TOR and each of the three proxies (nodes) you access encrypts your data. No individual node can know both what you are connected to and who you are. The third node decrypts the data and accesses the website, sending the information back through the proxies in encrypted form.*

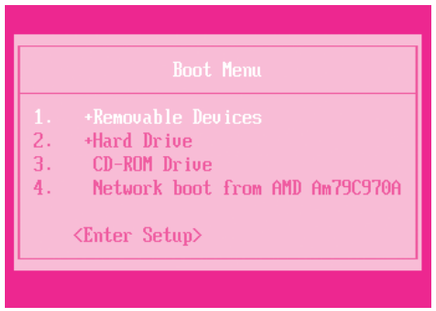
ii. *An Internal Protocol address is a string of numbers that allows you to send and retrieve data over an internet connection (for example, 78.125.1.209). This number identifies the location, Internet service provider, and technical details of your connection. It is comparable to a house's street address. An unobscured IP will lead investigators directly to your connection.*

iii. *The Media Access Controller address specifically identifies your computer. If you access the internet, the router may log your MAC address and maintain that log. If investigators were to read the logs of a router you accessed (say, a public wifi from which a communiqué was sent), and then compare that address with the MAC address of your computer's wireless card (say, confiscated in a raid), you'd be connected to your activity while using that router's connection. If the MAC address is not changed, there is the possibility of your activity being traced back to you if investigators are persistent or lucky enough.*



1 Download and install Tails

Tails can be downloaded at *tails.boum.org*. See 'Tails Installation Assistant' on the site for instructions on how to download and verify the file, install it on a USB or CD, and boot it on your computer.

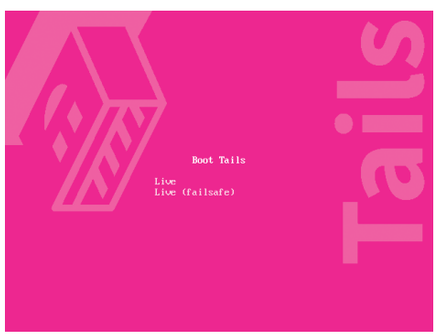


2 Boot Tails

Depending on how risky your activity is, it might be best to use a computer that isn't connected to your identity (in case Tails, for whatever reason, does leave a trace). This could be a public computer out of sight of surveillance cameras, or a laptop used specifically for this purpose.

If you start the computer with the USB plugged in, and Tails doesn't start automatically, you might have to access the 'boot menu' of your computer. On most computers, you can press a boot menu key to display a list of possible devices to start from (identify the potential boot menu keys for the computer depending on the computer manufacturer in the list below). In the boot menu, choose your USB. For troubleshooting, see 'Start Tails' at *tails.boum.org*. You may need to edit the BIOS settings.

Manufacturer	Key
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12,
Novo,	F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12



3 Connect to internet

If using a laptop, you can access many wifi networks with prior knowledge of the password from outside the building, even at night if they leave the wifi on. Use wifi that doesn't have a 'captive portal' (that makes you accept terms and conditions).

4 Submit Communique

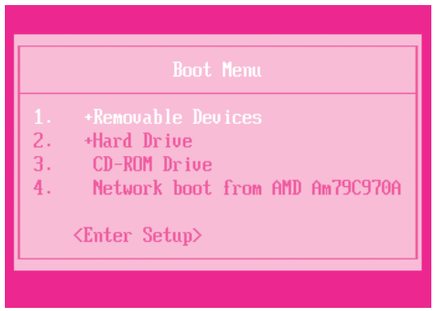
Open TOR browser, and verify TOR is functional by going to *check.torproject.org*. Visit *https://mtlcounter-info.org/add-content/* to send us your communique! If submitting any images, video, etc., remove identifying information (metadata) with the Metadata Anonymization Toolkit (MAT) on Tails.

More In-depth Resources:

- Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communications
- Anonymity/Security zine
- Surveillance and Counter-surveillance Guide

1 Download and install Tails

Tails can be downloaded at *tails.boum.org*. See 'Tails Installation Assistant' on the site for instructions on how to download and verify the file, install it on a USB or CD, and boot it on your computer.

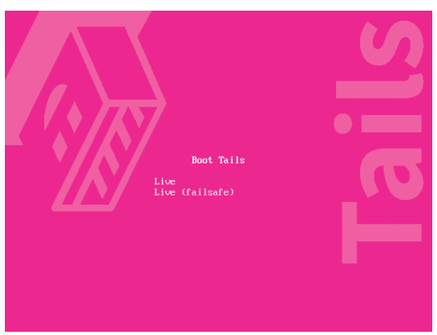


2 Boot Tails

Depending on how risky your activity is, it might be best to use a computer that isn't connected to your identity (in case Tails, for whatever reason, does leave a trace). This could be a public computer out of sight of surveillance cameras, or a laptop used specifically for this purpose.

If you start the computer with the USB plugged in, and Tails doesn't start automatically, you might have to access the 'boot menu' of your computer. On most computers, you can press a boot menu key to display a list of possible devices to start from (identify the potential boot menu keys for the computer depending on the computer manufacturer in the list below). In the boot menu, choose your USB. For troubleshooting, see 'Start Tails' at *tails.boum.org*. You may need to edit the BIOS settings.

Manufacturer	Key
Acer	Esc, F12, F9
Asus	Esc, F8
Dell	F12
Fujitsu	F12, Esc
HP	Esc, F9
Lenovo	F12,
Novo,	F8, F10
Samsung	Esc, F12, F2
Sony	F11, Esc, F10
Toshiba	F12



3 Connect to internet

If using a laptop, you can access many wifi networks with prior knowledge of the password from outside the building, even at night if they leave the wifi on. Use wifi that doesn't have a 'captive portal' (that makes you accept terms and conditions).

4 Submit Communique

Open TOR browser, and verify TOR is functional by going to *check.torproject.org*. Visit *https://mtlcounter-info.org/add-content/* to send us your communique! If submitting any images, video, etc., remove identifying information (metadata) with the Metadata Anonymization Toolkit (MAT) on Tails.

More In-depth Resources:

- Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communications
- Anonymity/Security zine
- Surveillance and Counter-surveillance Guide