irc.iranserv.com #iberoamerica

/dev/null antes que el deshonor

Anonymous – El Manual Super-Secreto

Compilado por Anonymous

Versión 0.2.1.2
Fecha: 9 de Abril de 2.011

Traducción y Adaptación: Junio de 2.011
0ark1ang3l, Busirako, EpicFail, GlynissParoubek
HADEXX, Joe_Yabuki, Opcode

Actualización Continua: Busirako

VERSIÓN DE BORRADOR

Puede contener errores tipográficos.
Contiene <°-(-(-(-<
No contiene (o) (o)
Ni 8====D
además, tl;dr

Apoyamos la libertad de expresión

Resumen para los impacientes.

Anonymous – Guía Introductoria Para la Seguridad en Momentos de Inestabilidad Social

Prólogo [pro1]

Activistas políticos, disidentes e incluso espectadores sin afiliación atrapados en situaciones de inestabilidad social temen con frecuencia por su protección y la de sus familias. En estas situaciones, los ciudadanos quizás enfrenten la oposición ruda y aun violenta de las autoridades y fuerzas de seguridad. Esta guía está diseñada para introducir al lector a la mentalidad requerida para mantenerse seguro durante disturbios y protestas tanto en línea como en el mundo físico. Además, intenta ayudar a establecer una comunicación continua en momentos en que Internet y las líneas telefónicas sean restringidas.

Índice [ind2]

Para ir a una sección de esta guía, use la opción de búsqueda de su computador [Windows: Ctrl+B / Macintosh: Command+F] e introduzca el código de cuatro caracteres que aparece junto a la sección en el índice. Por ejemplo, en Windows, para ir al prólogo, presione Ctrl+B y teclee "pro1" [sin las comillas].

Introducción [int3]

La primera sección de esta guía se concentrará en la seguridad personal. Puede hablarse de protección personal en dos aspectos diferentes: protección física y protección en internet. Es importante recordar que esos dos aspectos se sobreponen: un error de protección en internet puede llevar a la identificación física. Sin embargo, si tiene en cuenta unas pocas e importantes reglas, puede reducir considerablemente la posibilidad de ser individualizado e identificado.

La segunda sección de esta guía tratará temas tecnológicos específicos que pueden utilizarse para comunicarse anonimamente, mantener la confidencialidad y protestar de manera efectiva.

Nota de los traductores: Es importante tener en cuenta que la gran mayoría de la información relacionada en este documento como referencia se encuentra en inglés. Si no entiende este idioma, tiene dudas o requiere información adicional, póngase en contacto con algún operador o administrador en irc.iranserv.com #iberoamerica. Más adelante encontrará la información necesaria para hacerlo.

Protección Personal [prs4]

Protección Física [fis5]

La clave de la protección física está en actuar de modo normal para no llamar innecesariamente la atención sobre usted mismo ni revelar a nadie información que permita ser identificado. Los pasos para lograrlo pueden separarse en dos listas: "Qué hacer" y "Qué NO hacer". Estos pasos son especialmente importantes si usted es un activista, ya que esto lo pone en un lugar más riesgoso para empezar.

Qué hacer:

- Mézclese con la multitud
- Dispérsese entre los flujos de gente
- Mantenga un perfil bajo
- Esté al tanto de las noticias, en especial sobre los puntos de reunión de las protestas, los puntos de control o seguridad [de las autoridades] y los bloqueos de vías
- Busque señales de policías encubiertos
- Oculte todo aquello que pueda ser usado para identificarlo como tatuajes o cicatrices
- Si obtiene material de Anonymous o guías de protesta, intente compartirlos con los otros manifestantes; estos materiales pueden contener información importante sobre seguridad

Sugerencias adicionales para los manifestantes:

- Establezca canales seguros de comunicación con otros manifestantes
- Establezca los puntos de encuentro y reencuentro, así como un plan de escape, antes de llegar a la protesta
- Tenga más de un plan alternativo
- Busque comunicados de Anonymous y Telecomix y léalos

- Descargue la Guía de Disturbios de Anonymous (http://goo.gl/kQdwV) para hacer una máscara antigas casera, encontrar estrategias avanzadas de coordinación, etc.

Qué NO hacer:

- No confíe en que nadie sea quien dice ser
- No dé a nadie ningún tipo de información personal que pueda ser usada para identificarlo
- No mencione nada relacionado a sus relaciones personales, familiares o de sus allegados
- No mencione sus vínculos con grupos activistas
- No mencione el grupo Anonymous a nadie que no conozca
- No mencione nada respecto a su educación, empleo, etc.

Protección en Internet [int6]

Todo uso de internet puede ser potencialmente utilizado para localizarlo físicamente. Es importante no revelar información en la red. Si usted está dedicado a cualquier tipo de actividad controversial en línea, como discutir sobre protestas o postear en un blog sobre el tema, debe asegurarse de ocultar su dirección IP (ver la sección "Seguridad en Internet" [isc7]).

Qué hacer:

- Tenga en cuenta que cualquier interacción en línea puede ser vista por otros
- Piense en lo que hará antes de hacerlo: no diga nada que pueda lamentar, pues podría ser grabado o almacenado
- Cree nombres de usuario y contraseñas distintivos y seguros. Para ello, use letras, números y caracteres especiales
- Si le es posible, use una VPN (Virtual Private Network: Red Privada Virtual; ver [isc7])
- Borre las cookies, el historial y el caché de su navegador después de cada sesión en internet
- Use el modo de navegación privado o incógnito de su navegador siempre que le sea posible

- Use clientes como Firefox en lugar de Internet Explorer
- Use cuentas de correo temporales o desechables para crear sus cuentas de Facebook, etc. (ver [eml4])
- Use plugins de Firefox para obtener seguridad adicional (ver [ffx5])

Qué NO hacer:

- No use su nombre real completo ni parte de él en sus cuentas y nombres de usuario
- No mencione nada que pueda servir para identificarlo (ver [fis5])
- No mencione su zona horaria
- No mencione sus características o habilidades físicas
- No mencione nada acerca de sus relaciones personales, su familia o personas cercanas
- No se conecte/desconecte simultáneamente a/de servicios como Twitter o Facebook. Alterne su acceso de tal manera que no puedan relacionarse las cuentas de diferentes servicios.

Seguridad en Internet [isc7]

Cada dispositivo en línea tiene una dirección IP. Una IP se puede utilizar para ayudar a localizar físicamente a un individuo. Por esta razón, es importante ocultar su IP. Hay muchas maneras de hacer esto. Usted debe utilizar tantas capas de seguridad como sea posible en un momento dado para aumentar su protección. Prepare los métodos de la seguridad de Internet con anterioridad en caso de que se presente repentinamente alguna restricción en el acceso a Internet. Los tres métodos principales que serán discutidos en este artículo son VPNs, I2P y proxies.

Red Privada Virtual (VPN) [vpn8]

Una Red Privada Virtual o VPN (siglas en inglés de Virtual Private Network) es un método para asegurar la información que se transmite por internet. Al escoger un servicio de VPN, intente que éste sea provisto por un país que no va a compartir su información privada fácilmente. Por ejemplo, los servicios de Islandia o Suiza son más

seguros que un servicio de los Estados Unidos. También intente encontrar un servicio que no guarde información de usuario o información de pagos (si se usa un servicio de pago).

Guías para instalar el servidor de OpenVPN:

- Windows: http://www.vpntunnel.se/howto/installationguideVPNtunnelclient.pdf
- Linux (Basado en Debian): http://www.vpntunnel.se/howto/linux.pdf
- Mac: http://www.vpntunnel.se/howto/mac.txt

Servicios de VPN gratuitos [No recomendados]:

- http://cyberghostvpn.com
- http://hotspotshield.com
- http://proxpn.com
- http://anonymityonline.org

Servicios de VPN comerciales [Recomendados]:

- http://www.swissvpn.net
- http://perfect-privacy.com
- http://www.ipredator.se
- http://www.anonine.se
- http://www.vpntunnel.se

Descargas gratuitas de VPN [No recomendadas]:

- Windows: HotspotShield - http://hotspotshield.com
  UltraVPN - https://www.ultravpn.fr/download/ultravpn-install.exe
- Mac: UltraVPN - https://www.ultravpn.fr/download/ultravpn.dmg
- Linux: UltraVPN - https://www.ultravpn.fr/forum/index.php?topic=204.0

I2P [i2p9]

I2P es una red para “anonimizar” que soporta varias aplicaciones seguras. Recomendamos usar pchat para conectarse a anonworld.net y unirse a canales como #iberoamerica.

Páginas web de I2P:

- http://geti2p.net
- http://i2p2.de

Video tutorial de I2P para Windows:

- https://www.youtube.com/watch?v=5J3nh1DoRMw

Video tutorial de I2P para Linux:

- https://www.youtube.com/watch?v=QeRN2G9VW5E

Sitios de I2P activos:

- http://inr.i2p

Utilización de puertos I2P:

- http://www.i2p2.de/faq#ports
- Ver también la configuración de su enrutador

Cómo instalar y ejecutar I2P en Linux

- Descargue y extraiga los archivos de instalación, no hay necesidad de instalarlos separadamente (como instalación de apt-get).
- Ejecute el router desde la carpeta /i2p con "sudo sh i2prouter start". En segundos, I2P debería abrir una página web en Konqueror (o el navegador por defecto) con la consola principal de I2P.

- Configure sus ajustes de ancho de banda. También debería considerar abrir algunos puertos de su firewall para optimizar el uso del ancho de banda.

I2P Portable (Solo Windows)

- http://portable-i2p.blogspot.com
    - Contiene I2P, varios complementos, buscador pre configurado, cliente de IRC pre configurado y mensajería instantánea.
    - Antes de que pueda utilizar algún servicio con I2P, tiene que iniciar el enrutador de I2P desde el menú de portableapps con el botón "I2P Launcher".

Navegación anónima con I2P

- Diríjase a opciones o preferencias de su navegador y de allí a configuración de red
- Seleccione "configuración manual del proxy"
- En "http" digite 127.0.0.1, en "puerto" digite 4444
- En "https" digite 127.0.0.1, en "puerto" digite 4445

Asegúrese de que en donde dice "No usar proxy para" diga "localhost, 127.0.0.1" para que pueda tener acceso a la página de configuración de I2P. Para probar su anonimato, vaya por ejemplo a: cmyip.com

Proxies [prx0]

Los proxies son conexiones intermediarias que pueden ayudar a ocultar su IP. Estas no encriptan los datos. También pueden ayudar a acceder a sitios web restringidos. Utilícelas junto con los servicios de VPN para incrementar su seguridad. Vea también los siguientes enlaces y la sección [tor2]:

- http://www.freeproxies.org
- http://www.socks24.org
- http://www.samair.ru/proxy

Tor Onion Router [tor1]

Tor es una red de proxies que ayuda a ocultar su IP. Esta NO encripta datos. Algunos países específicos (como Irán) afirman haber evitado la protección de Tor

Descarga de Tor:

- https://www.torproject.org

Descarga del botón de Tor para Firefox (Activar/desactivar Tor en el navegador):

- https://www.torproject.org/torbutton

Tor viene incluido también en el Paquete de Protección Anonymous [pkg6]

Comunicaciones [cmm2]

Anonymous alienta a los ciudadanos de los países en protesta a solicitar asistencia. La mejor forma de hacerlo es utilizando IRC para conectarse a #iberoamerica. Por favor recuerde que es más seguro utilizar una VPN [vpn8] o I2P [i2p9]. Puede conectarse a IRC a través del link en anonhispano.blogspot.com.

En el evento de una caida de Internet, puede estar seguro de que Anonymous y Telecomix harán todos los esfuerzos necesarios para restaurar las comunicaciones. Hay algunas cosas en las que puede ayudar:

- Trate de conectarse a Internet desde diferentes ubicaciones, algunas veces solo algunas ISPs dejan de operar mientras que otras permanecen operativas.
- Trate de utilizar conexiones dial-up (modem) de ser posible.

- Ubique radio-aficionados y escuche comunicaciones de grupos como Telecomix, ellos están en capacidad de proveer instrucciones para métodos de conexión alternativos a Internet.
- Ubique universidades y oficinas con equipos de fax, estos equipos pueden ser utilizados como medio de comunicación de una sola vía para proveer actualizaciones y material inspiracional.

Información Adicional [add3]

Cuentas de Correo Temporales / Desechables [eml4]

Se pueden crear cuentas de correo rápidamente en los siguientes sitios:

- http://10minutemail.com
- http://www.sofortmail.de
- http://www.trashmail.com
- http://www.guerrillamail.com
- http://www.spam.la

Se puede encontrar un proveedor de correo que enfatiza en la seguridad en: http://hushmail.com [no recomendado, mantiene información por si el gobierno la solicita].

Plugins / Extensiones Útiles para Firefox [ffx5]

- BetterPrivacy - Remueve las cookies persistentes de los componentes de flash.
- NoScript - bloquea Javascript.
- Ghostery - Detecta pixeles de seguimiento.
- GoogleSharing - GoogleProxy para sitios en donde Google está censurado.
- User Agent Switcher - Envía a los servidores información errónea de la identidad del navegador.

- Optimize Google - Remueve la información que Google utiliza para rastrear las búsquedas.
- Outernet Explorer (MacOS) - Crea numerosas búsquedas para prevenir la captura de paquetes.
- https://www.eff.org/https-everywhere - Automáticamente carga https en un sitio si está disponible.
- Scroogle SSL search (Búsqueda anónima en Google) - https://ssl.scroogle.org

Paquete de Protección Anonymous [pkg6]

Anonymous provee un Paquete de Protección actualizado frecuentemente que contiene guías y software de utilidad. La mejor manera de obtenerlo es entrar a IRC y solicitarlo. A IRC se puede acceder desde anonworld.net y puede encontrar asistencia en canales como #iberoamerica [/join #iberoamerica]. Por favor tenga en cuenta protocolos de seguridad como la utilización de VPN [vpn8] o I2P [i2p9] al entrar a IRC.

Fin del resumen para los impacientes

Prefacio

Las más grandes amenazas a su seguridad son: A) ingeniería social y su comportamiento y B) revelar su dirección IP.

Para A) vea Amenazas Sociales

Para B) vea Técnico

Trate de seguir la mayor cantidad de estas sugerencias que le sea posible para asegurar la máxima seguridad

Amenazas Sociales

Regla básica: mézclese con la multitud, disperse panfletos en diferentes secuencias. Mantenga un perfil bajo. No trate de ser especial. Recuerde, cuando esté en Roma, actúe como Romano. No trate de ser un culo inteligente. Los policías son muchos, Anonymous es Legión, pero usted es sólo uno. No hay héroes viejos, sólo hay héroes jóvenes y héroes muertos.

- no de información personal en el chat IRC porque es público. Su mamá podría leer lo que escribe allí y también la policía y no mencione su participación en Anonymous en la vida real.
- no incluya información personal en su nombre de pantalla.
- no facilite su información personal, su dirección o de dónde es usted.
- no mencione su género, tatuajes, cicatrices, piercings u otras características físicas llamativas
- +/- peso al normal, (in)habilidades físicas o psicológicas (¿Se hace una idea?).
- no mencione su profesión, hobbies o aficiones.
- no mencione si tiene una relación sentimental.
- no mencione su participación con otros grupos activistas.

- preferencias musicales o gustos literarios y películas son una buena manera de conocer a alguien, no mencione ninguno de los suyos.
- no utilice caracteres especiales, que son existentes sólo en su idioma porque revelarían su ubicación.
- no de información ni siquera falsa. Algunos pueden tratarla como verdadera.
- todo debe estar completamente separado entre su vida real y su vida en línea
- nada de su vida real debe mezclarse con Anonymous, no hable sobre Anonymous en la vida real excepto para publicar carteles anónimamente, etc.
- no mencione congresos en los que usted ha estado.
- no mencione su escuela, universidad, etc..
- no mencione qué hora es en el país en el que vive, mencionando la hora se puede revelar dónde vive.
- no se conecte siempre a la misma hora. Intente hacerlo de forma alternativa.
- no publique en la red mientras esté en IRC y definitivamente no mencione que está publicando algo en Twitter. Esto es fácil de correlacionar
- no mencione si está personalmente realizando un ataque DDoS, escribiendo algún procedimiento o realizando un escaneo con Nmap al objetivo, ni si está haciendo gráficos, etc. Solamente discuta la estrategia general.
- no envíe imágenes alojadas en Facebook. El nombre del archivo contiene el ID del perfil.
- sus inicios de sesión y cierre en Facebook, Twitter e IRC, pueden ser comparados y asi identificarle.

Técnico

Regla básica: Utilice tantas capas de seguridad como sea posible. La cuestión no es que usted sea paranoico, es qué tan paranoico es usted.
Un buen inicio es utilizar una VPN y ejecutar software relacionado con Anonymous desde un dispositivo USB o un Live CD. Un proxy también puede servir pero no es tan seguro como una VPN.

Siempre utilice tantas capas de seguridad como sea posible. Asegúrese de utilizarlas como debe ser. Si no sabe cómo hacerlo, aprenda antes de hacerlo.
La mayoría de Anonymous utiliza una VPN para esconder sus rastros, utilizan conexiones encriptadas con SSL y #vhost cuando están en irc.iranserv.com.

VPN

Al pensar en un servicio de VPN, hágalo primero con la legislación del país que ofrece el servico. Una VPN de EE.UU. podría proporcionar sus datos de usuario al ser solicitados por las autoridades. En otros países como Suecia o Islandia es poco probable que suceda. Tienen una fuerte política de privacidad, lo que les hace más difícil a las agencias de aplicación de la ley el obtener acceso a sus información. Adicionalmente, algunos servidores no mantienen registros de los usuarios. También trate de conseguir servicios de VPN que acepten pagos anónimos (Algunos mantienen la información de facturación).

Más información: https://secure.wikimedia.org/wikipedia/es/wiki/VPN

Guía para la instalación del cliente OpenVPN

(tomado de las FAQ de vpntunnel.se)

- Windows: http://www.vpntunnel.se/howto/installationguideVPNtunnelclient.pdf
- Linux (basado en Debian): http://www.vpntunnel.se/howto/linux.pdf
- Mac: http://www.vpntunnel.se/howto/mac.txt

VPN Gratuitas - No recomendadas (ver explicación)

Si no le venden un servicio lo están vendiendo a usted.

- http://cyberghostvpn.com
- http://hotspotshield.com

- http://proxpn.com
- https://anonymityonline.org

Proveedores comerciales de VPN

- http://www.swissvpn.net
- http://perfect-privacy.com
- https://www.ipredator.se
- http://www.anonine.se
- https://www.vpntunnel.se

Descargas directas de VPN -- No recomendadas (ver explicación)

Si no le venden un servicio lo están vendiendo a usted.

Mac

- Ultra VPN: https://www.ultravpn.fr/download/ultravpn.dmg

Linux

- UltraVPN: https://www.ultravpn.fr/forum/index.php?topic=204.0

Windows

- HotspotShield: http://hotspotshield.com
- UltraVPN: https://www.ultravpn.fr/download/ultravpn-install.exeSoftware

Explicación

1.- VPN Gratuita: No se recomienda porque muchas características son limitadas y, adicionalmente, muchos proveedores de VPN gratuitas pueden suministrar información ante solicitud de las autoridades. Además, muchas VPNs gratuitas trabajan con compañías de publicidad.

2.- PPTP Comercial: Tal como Telecomix lo ha mencionado, algunos sistemas operativos (Windows 7, Vista) pueden ser vulnerables a ataques que requieren conexiones p2p lo que puede llevar al atacante a conocer su verdadera IP.
Ver https://www.ipredator.se/?lang=en para más información sobre este tema. Al parecer, la falla tiene que ver con las conexiones IPv6 así que asegúrese de utilizar solamente IPv4.
3.- VPNs Recomendadas. Todas las que utilicen el servicio OpenVPN. Esto incluye políticas específicas sobre el resguardo de información del usuario y sobre los datos. (La mejor opción es: no registro de datos + no registro de facturación + métodos seguros de pago = Ukash o servicios similares).

Red de Anonimización I2P

I2P es una red de anonimización que ofrece una sencilla capa que las aplicaciones sensibles a la identidad pueden utilizar para comunicarse de forma segura. Todos los datos son empaquetados en múltiples capas de encripción y la red es distribuida y dinámica, sin partes de confianza.
Hay disponibles muchas aplicaciones que interactúan con I2P incluyendo correo, P2P, IRC, mensajería instantánea y otras. Todas anónimas.

Asegúrese de empezar iniciando I2P con el botón I2P Launcher en el ícono de bandeja de las aplicaciones portables.
Puede utilizar entonces el cliente Pchat incluido que, automáticamente, se conecta al servidor IRC de I2P anónimamente.
Entre a #iberoamerica para mantenerse al tanto de las actividades de Anonymous. Muchos canales de operaciones retransmiten entre I2P y anonworld.net.
Disfrute de su anonimato y privacidad!

Sitios Web:

- http://geti2p.net
- http://i2p2.de

Video Tutorial de I2P para Windows:

- https://www.youtube.com/watch?v=5J3nh1DoRMw

Video Tutorial de I2P para Linux:

- https://www.youtube.com/watch?v=QeRN2G9VW5E

Video - Cómo configurar su propio sitio web en I2P:

- https://www.youtube.com/watch?v=2ylW85vc7SA

IRC con I2P:

- 127.0.0.1:6668
- Canal: #iberoamerica
- Sitios: (actualmente sin respuesta) anonops.i2p qr.i2p
- Telecomix IRC permite entunelamiento I2P

Para más sitios I2P activos visite:

- http://inr.i2p

Puertos que utiliza I2P:

- http://www.i2p2.de/faq#ports
- Vea también la configuración de su enrutador.

Instalación y ejecución de I2P en Linux:

- Descargue y extraiga los archivos de instalación. No hace falta una instalación separada como apt-get install.

- Ejecute el enrutador desde la carpeta /i2p con: "sudo sh i2prouter start". En segundos, I2P abrirá una página con la consola principal de I2P en el navegador Konqueror o en su navegador por defecto.
- Realice la configuración de ancho de banda. Debe considerar también abrir algunos puertos en su firewall para optimizar la utilización de su ancho de banda.

I2P Portable (solo Windows):
Contiene I2P, variados plugins (email, torrentclient), navegador preconfigurado, IRC preconfigureado IRC client y messenger.

- http://portable-i2p.blogspot.com

Antes de poder utilizar cualquier servicio en I2P deberá iniciar el enrutador I2P desde el ícono de la bandeja de portableapps con el botón I2P Launcher.

Navegación anónima con I2P:

- Seleccione la opciones/preferencias dependiendo de su navegador
- Seleccione Configuración de red/conexión
- Seleccione Configuración de proxy manual
- En http digite 127.0.0.1 , en puerto digite 4444
- En https digite 127.0.0.1, en puerto digite 4445

Asegúrese de no tener un proxy para localhost, 127.0.0.1 si no, no podrá acceder a la página de configuración de I2P. Para probar su anonimato, visite cmyip.com.

Tor Onion Router

Regla Básica: Tor no encripta los datos que usted envía. Simplemente esconde su IP a través de una cascada de proxies. Instalar Tor no significa que usted esté seguro. Por ejemplo, si utiliza Tor y se valida en su cuenta de correo real, personal, estará muy [jodido].

Descargue Tor:

- https://www.torproject.org

Descargue Torbutton para Firefox (habilitar o deshabilitar el uso de Tor en el navegador):

- https://www.torproject.org/torbutton

Anonymous provee el llamado Paquete de Protección. Contiene Tor así como otras cosas útiles. Si no puede acceder al sitio web de Torproject, puede solicitar en los canales de IRC el Paquete de Protección Anonymous.

Instrucciones para IRC

Regla Básica: Utilice el puerto SSL (en este caso 6697). Siempre. Use #vhost. Siempre. IRC es público, si no quiere que la información se reparta públicamente, en primer lugar, no la suministre. Ignore a los trolls. Siempre.

Qué es IRC? IRC es un programa gratuito de conversación que la gente en todo el mundo puede utilizar para comunicarse. Tiene múltiples canales para diferentes temas de conversación y mensajería privada entre usuarios.

Cuando se conecte a la red IRC de Anonymous, hágalo solamente vía SSL (apunte su cliente al puerto 6697). El puerto 6697 es un puerto SSL no muy común. Simplemente marcar la opción de "Siempre utilizar SSL" no funcionará. Al conectarse al puerto SSL 6697 su cliente IRC puede darle un mensaje de advertencia ya que el certificado SSL está auto-firmado. No es problema, puede confiar en este certificado.

Después de conectarse, registre su apodo (nick) utilizando una dirección de correo falsa, entre al canal #vhost (/join #vhost) y DESPUÉS de este procedimiento, podrá unirse a los canales.

Lista Básica de Comandos IRC:

/join #nombredelcanal	Entra al #nombredelcanal
/part	Sale del canal activo
/query Nick	Abre una conversación privada con nick
/msg nick <mensaje>	Envía un mensaje privado a nick
/whois Nick	Muestra información sobre nick
/msg nickserv identify <password>	Identifica su nick
/ignore <nick>	Ignora un troll
/topic	Para ver el tema del canal
/list	Lista todos los canales activos

Comandos extendidos:

- http://www.ircbeginner.com/ircinfo/m-commands.html

Dónde encontrar información sobre IRC en caso de no poder conectarse:

- http://anonhispano.blogspot.com/p/chat.html (Carga un cliente IRC basado en web con toda la información necesaria para conectarse)

Seguridad:

- Utilice SSL para conectarse a IRC. El puerto del servidor es 6697.
- Utilice software de VPN o cuentas que escondan su IP. Los servidores IRC son seguros pero no invulnerables. Tor NO es una opción (Está bloqueado en la red por abuso malintencionado).

La seguridad adicional consiste en obtener un vhost (Host Virtual):

- Registre su nick: /msg nickserv register contraseña email@falso.com

- /join #vhost
- estando en #vhost escriba: !vhost cualquier.host.falso

Clientes IRC

Mac

Descargue Colloquy desde:

- http://colloquy.info/downloads/colloquy-latest.zip
- http://files5.majorgeeks.com/files/aaea265a9054b3b8c5df99c64685ec2e/mac/messaging/colloquy-latest.zip

Utilice un proxy web como alguno de los siguientes. Asegúrese de conectarse a través de SSL. ("direccionip:puerto")

- 62.112.33.2:80
- 200.125.243.122:8080
- 120.39.24.156:808
- 58.22.151.6:80
- http://www.proxy-list.org/en/index.php?pp=any&pt=2&pc=any&ps=y&submit=Filter+Proxy

Utilización:

- Inicie Colloquy
- Haga click en New
- Escriba un nickname (nunca su verdadero nombre)
- Entre a un servidor de Chat, para nuestros propósitos, irc.iranserv.com.
- Haga click en Details
- Seleccione el Secure Web proxy y marque la opción SSL option, use el puerto 6697

- No ponga su nombre real en User ni en Real Name, invéntese algo.
- Si lo desea, haga click en: Remember Connection
- Oprima Connect
- Haga click en Join Room y entre al Chat Room #iberoamerica, por ejemplo.

Linux

Xchat (Gnome)

- Debian/Ubuntu/Knoppix... : sudo apt-get install xchat
- Redhat/Fedora(64bit only): http://www.xchat.org/files/binary/rpm
- Gentoo: sudo emerge --sync | sudo emerge -av xchat

Utilización:

- Inicie X-Chat
- Haga click en el botón de Add de la lista de redes y nómbrela como quiera.
- Haga click en el botón de Edit en la red seleccionada, cambie la entrada de newserver/6667 a irc.iranserv.com/6697 (o utilice uno de los nuevos dominios que encontrará listados más adelante).
- Seleccione las dos opciones de Use SSL for all servers on this network y Accept invalid SSL certificate.
- Haga click en Close y entre a http://konversation.kde.org

Konversation (KDE):

- Debian/Ubuntu/Knoppix... : sudo apt-get install konversation

Utilización similar a X-Chat

Windows

X-Chat2

- Versión Libre: http://www.silverex.org/download

- Mirror: http://download.cnet.com/X-Chat-2/3000-2150_4-10972145.html

XChat:

- http://xchat.org/download

Mirc:

- http://www.mirc.com/get.html

Utilización:

- Descargue las librerías SSL: http://www.mirc.com/download/openssl-0.9.8q-setup.exe
- Instálelas bien sea en la carpeta de mIRC (C:\Program Files\mIRC o C:\Program Files(x86)\mIRC) o en la carpeta de sistema de Windows (C:\Windows\System32).
- Al ejecutar mIRC, éste debe utilizar las librerías OpenSSL automáticamente. Para confirmar que mIRC las ha cargado, abra el diálogo de Options y verifique en la sección Connect/Options que el botón de SSL esté habilitado.
- Digite /server irc.iranserv.com:6697

Basado en Web

http://01.chat.mibbit.com

- En la página de mibbit, haga click en server y en el campo digite: irc.iranserv.com:+6697
- Cómo saber si funciona? Escriba /whois su_nick y deberá recibir un mensaje que dice que su conexión es segura.

http://anonhispano.blogspot.com/p/chat.html

Instrucciones Vhost

En los servidores Anonymous de IRC se puede solicitar un Vhost. Esto asegura que usted sea anónimo en la red IRC. Por defecto, usted obtendrá un host basado en su ISP, algo como:
minick@theservicefrom.125.comcast.suck.net o un hash si se ha conectado por SSL:
minick@6969E1A1T1COCK152.69.IP.
Después de seleccionar su vhost deseado usted podrá ser identificado como: minick@myvhostRocks.org.

1.- Deberá tener un nick registrado para acceder a un vhost.

- Digite /msg nickserv register password fake@email.com

Explicación: Este comando le dirá al servicio de registro que reserve su nick para futuros usos.

2.- Deberá identificarse con su nickname para que el vhost funcione.

- Digite: /msg nickserv identify password.

Explicación: Una vez usted ejecute este comando estará listo para configurar un vhost.

- Respuesta: services.anonworld.net sets mode +r Sunick

Explicación: La marca +r demuestra que un determinado nick ha sido efectivamente registrado e identificado.

3.a- Entre al canal #vhost para configurar el servicio.

- Digite (en el canal): !vhost host.falso.aqui

Explicación: Luego de solicitar el vhost el servicio bloqueará su nick en ese canal por un determinado tiempo. Las razones son varias, alguien podría obtener su verdadera IP, cambiar de vhosts cada 2 segundos podría poner lento el servidor, etc..

3.b.- Eventualmente usted podría solicitar un vhost por comando sin necesidad de entrar al canal.

- Digite: /hs request vhost@host.aqui

Explicación: No hará falta entrar al canal pero no es suficiente para que funcione.
La parte de vhost@ es opcional, la parte importante es host.aqui.

Considerando la explicación anterior, utilice el siguiente comando: /hs request host.aqui

- Digite: /hs on

Explicación: Este comando activará el vhost.

Problemas con Vhost:

P: Yo registré mi vhost pero cuando me conecto no se activa.
R: Ya se identificó con su nick? Usted obtendrá su vhost una vez su nick sea identificado. Repita el paso 2.

P: Acabo de cambiar mi vhost pero este aun no se aplica, por qué?
R: Usted necesitará actualizar su estado para que el cambio sea efectivo. Digite: /msg nickserv update

- Respuesta: HostServ- Your vhost of host.aqui is now activated.
- Respuesta: NickServ- Status updated (memos, vhost, chmodes, flags

Una vez realice estos pasos deberá obtener un vhost completamente operativo.

Analizando su Interred

Glasnost: Brindando Transparencia a Internet
"Las ISPs han incrementado la implementación de una gran variedad de hardware intermedio (Ej. firewalls, administradores de tráfico, filtros y redireccionadores) para monitorear y manipular el desempeño de las aplicaciones de los usuarios."

- http://broadband.mpi-sws.org/transparency

GTNOISE Network Access Neutrality Project
"NANO identifica degradaciones en el desempeño que pueden dar como resultado una violación a la neutralidad de la red generada por un Proveedor de Servicios de Internet (ISP), como un tratamiento diferente para determinado tipo de aplicaciones, usuafrios o destinos"

- http://www.gtnoise.net/nano

El Analizador de Red ICSI
"Qué está pasando con su red? Algunos servicios parecen no funcionar? Parece estar muy lenta? Hay algo mal?"

- http://netalyzr.icsi.berkeley.edu

Lo que está mostrando su navegador

"BrowserSpy.dk es el sitio en el que Usted puede ver qué tanta información revela su navegador acerca de usted y de su sistema".

- http://browserspy.dk

Qué tan único y rastreable es su navegador?
"Panopticlick prueba su navegador par aver qué tan única es la información que comparte con los sitios que se visitan".

- http://panopticlick.eff.org

Esye sitio web está censurado?
"Alguna vez se ha encontrado con un sitio web al cual no puede accede y se ha preguntado: Solo me pasa a mi? Herdict Web acumula reports de sitios a los que no se puede acceder".

- http://www.herdict.org/web

Seguridad General al Navegar

Regla Básica: Siempre navegue en "modo privado" de manera que queden menos pistas de su historial de navegación en su disco duro. Opera, Chrome, Firefox, Safari e Internet Explorer incluyen opciones de navegación privada.

Utilice una VPN gratuita, en la mayoría de los casos, asegura la privacidad en línea. Si es posible, utilice almacenamiento USB. Podrá destruirlo de ser necesario y no deja pistas en su disco duro.

Utilice una VPN distinta para cada uno de sus diferentes perfiles en línea. Cuando verifique sus cuentas de correo o Facebook reales, utilice una VPN distinta a la que usa para las actividades Anonymous.

Recicle sus cuentas en línea cuando sea necesario. Un nombre virtual es simplemente eso, algo que la gente utiliza para referirse a usted en determinadas situaciones.

Cuando cree cuentas, utilice una VPN o TOR, esto le dará un origen falso. Igualmente, utilice emails desechables.

Plugins/extensiones útiles (obligatorias) para Firefox

- BetterPrivacy (Remueve las cookies persistentes generadas por flash >> *.sol)
- NoScript (bloquea Javascript)
- AdBlock Plus (bloquea publicidad) (Suscríbase a las listas Easylist y Fanboy)
- Element Hider for Adblock Plus
- Ghostery (pixeles de rastreo)
- TACO (más bloqueo de publicidad)
- Redirect Controller
- Refcontrol

- WorldIP (conozca su pais, conozca sus derechos)
- Flagfox
- GoogleSharing (GoogleProxy, algunos lo utilizan ya que Google está censurado en sus paises, anonimiza las búsquedas) - Scroogle.org es también una muy buena alternativa
- User Agent Switcher envía información errada sobre la identidad del navegador a los servidores
- Optimize Google (permite bloquear la basura que Google utiliza para rastrear las búsquedas)
- Outernet Explorer (MacOS) (busca una grandísima cantidad de basura en la red cada 10 segundos de manera que si alguien captura sus paquetes encontrará muchísima información inutil)
- https://www.eff.org/https-everywhere (automáticamente carga https en un sitio si es que está disponible)
- Scroogle SSL search (búsqueda anónima en Google): https://ssl.scroogle.org

Seguridad del Sistema

Regla Básica: La seguridad es un proceso continuo no un estado. Realice auditorías periódicas de una forma regular y programada y haga copias de seguridad encriptadas. Los respaldos son importantes. Hay dos tipos de personas: los que tienen copias de seguridad y los que perdieron su información.

- Utilice un sistema operativo con el que esté familiarizado (en cualquier caso, Linux y Unix son mejores)
- Desinstale todo lo que no necesite
- Deshabilite todas las herramientas remotas
- Destruya o encripte /temp, /var/temp y cualquier archivo con acceso de lectura pública
- Encripte su disco duro (Truecrypt: www.truecrypt.org)
- Debian y otras distribuciones ofrecen encripción del disco duro en la instalación. Utilícela.
- Utilice una distribución que arranque desde un DVD/CD/USB
- Nunca mantenga registros
- Cierre todos los servicios innecesarios

- Utilice un firewall
- Los sitios de acceso público son perfectos (casi). (Se puede correlacionar el inicio de sesión con el CCTV). Se deben evitar las cámaras cuando se usen los accesos gratuitos. Cyber-cafés, Mc Donalds y otras compañías ofrecen acceso gratuito a Internet, recuerde no navegar desde estas redes sin utilizar una VPN y/o Tor.
- Mantenga sus llaves privadas (pgp/gnupgp) en un dispositivo removible y, este dispositivo, alejado de ojos curiosos. Encripte la llave privada antes de hacerlo.
- Mantenga los certificados de VPN alejados de ojos curiosos, en un dispositivo removible o en carpetas ocultas.
- Nunca utilice el mismo usuario y contraseña al reinstalar. Tómese el tiempo de crearlos nuevamente en cada oportunidad. Utilice generadores de contraseñas.
- Sea paranoico. Cualquier actividad extraña en su computador debe ser verificada y monitoreada. Esto provee dos cosas: conocimiento cuando se identifica y seguridad adicional.

Detectar potenciales fallos de seguridad en *Nix:
Sea cuidadoso si no sabe cómo leer los resultados de Lynis, se puede volver muy paranóico.

- http://www.rootkit.nl/projects/lynis.html

Scanner para rootkits, backdoors y exploits locales en *Nix:
De nuevo, si no sabe cómo leer los resultados de Rootkit Hunters se volverá paranóico

- http://www.rootkit.nl/projects/rootkit_hunter.html

Destrucción segura de información

Unix/Linux:

Para destruir información de una manera segura en *Nix hay varias posibilidades. El comando shred -u sobreescribe archivos individuales para finalmente eliminarlos. Con wipe -rcf se sobreescriben y eliminan directorios. Sea cuidadoso ya que la información destruida/eliminada no puede ser recuperada.

Abra una terminal y digite

- shred -u <archivo>
- wipe -rcf <directorio>

Si siente la necesidad de eliminar todo el disco duro, utilice el siguiente comando para discos IDE (/dev/hda es el primer disco)

- wipe -kq /dev/hda

Para discos SATA y SCSI digite (/dev/sda es el primer disco)

- wipe -kq /dev/sda

SI no está disponible wipe, se puede utilizar dd. (nuevamente para el primer disco)

- dd if=/dev/zero of=/dev/hda
- dd if=/dev/urandom of=/dev/hda

Utilice ambos comandos, uno después del otro. Si es especialmente paranóico, hágalo varias veces.

Mac:

Paquete de Privacidad Anonymous para Usuarios Mac. Incluye un eliminador seguro de documentos secretos y encripción AES-256
Herramienta de encripción (y algunos diseños extras)

- http://www.megaupload.com/?d=L2VQBEFE
- http://www.mediafire.com/?1xmu0m8jpy9b2a1

MD5 (Anonymous-MacPackage-Privacy.dmg) = 36e9ea524a86b94a451577ca46d3e15f

Windows:

AxCrypt http://www.axantum.com/AxCrypt

Las protestas no violentas (compilado desde: http://www.aeinstein.org/organizations103a.html)

Declaraciones Formales
Discursos públicos
Cartas de oposición o apoyo
Declaraciones de organizaciones e instituciones
Firmado de declaraciones públicas
Declaraciones de acusación y intenciones
Grupo o peticiones de masas

Comunicaciones con un público más amplio
Lemas, caricaturas y símbolos
Banderas, carteles y comunicaciones mostradas
Libros, folletos y panfletos
Periódicos y revistas
Registros, radio y televisión
Skywriting y earthwriting

Presiones sobre las personas
Funcionarios "Obsesionantes"
Burlándose de los funcionarios
Fraternización
Vigilias

Actos públicos simbólicos
Muestra de banderas y colores simbólicos
Uso de símbolos
Oración y culto
Entrega de objetos simbólicos
Protesta disrobings
Destrucción de propiedad
Luces simbólicas
Muestra de retratos
Pintura como protesta
Nombres y nuevos signos
Sonidos simbólicos
Reclamaciones simbólicas
Gestos groseros

Representaciones de grupo
Diputaciones
Simulacro de premios
Grupo de presión
Piquetes
Elecciones simuladas

Drama y Música
Sátiras y jugarretas humorísticas
Ejecución de obras de teatro y música
Cantando

Procesiones
Marchas

Desfiles
Procesiones religiosas
Peregrinaciones
Caravanas

Retirada y renuncia
Paros
Silencio
Renunciar a los honores
Dar la espalda

Honrar a los Muertos
Políticos de luto
Simulacro de funerales
Funerales Demostrativos
Homenaje a los lugares de entierro

Reuniones públicas
Asambleas de protesta o apoyo
Protesta reuniones
Mítines de protesta
Teach-ins

Los métodos de no cooperación social

El ostracismo de las personas
Boicot Sociales
Boicot sociales selectivos
Lysistratic no acción
Excomunión
Prohibir

No cooperación con eventos sociales, costumbres e instituciones.
Suspensión de actividades sociales y deportivas
Boicot de los asuntos sociales.

Huelga de Estudiantes
Desobediencia Social
Retirada de las instituciones sociales.

Retirada del sistema social
Estancia-en-casa
Falta de cooperación personal total
"Vuelo" de los trabajadores
Santuario
Desaparición colectiva
La emigración de protesta (hijrat)

Los métodos de no cooperación económica: (1) el boicot económico

Acciones de los Consumidores
Boicot de los consumidores
No consumir productos boicoteados
Política de austeridad
Retención del alquiler
La negativa a alquilar
Boicot de los consumidores nacionales
Boicot de los consumidores internacionales

La acción de los Trabajadores y Productores
Boicot por accidentes del trabajo
Boicot de los productores

La acción de intermediarios
Boicot a proveedores y manipuladores

La acción de los propietarios y directores.
Boicot de los comerciantes
Negativa a dejar o vender propiedad
Cierre patronal
Denegación de asistencia industrial
"huelga general" de los comerciantes

Medidas adoptadas por los titulares de Recursos Financieros
La retirada de los depósitos bancarios
Negativa a pagar honorarios y cuotas
La negativa a pagar deudas o intereses
Recorte de fondos y de crédito
La negativa a realizar nuevos ingresos
La negativa de dar dinero para el gobierno

Acción por los gobiernos
Embargo doméstico
Listas negras de comerciantes
Embargo de los vendedores internacionales
Embargo de los compradores internacionales
Embargo comercial internacional

Los métodos de no cooperación económica: (2) La huelga

Las huelgas simbólicas
Huelgas Protesta
Huelgas Relámpago

Las huelgas agrícolas
Huelga de Campesinos

Huelga de los trabajadores agrícolas

Las huelgas de los Grupos Especiales
Huelga de jornaleros reclutados
Huelga de los presos
Arte de la huelga
Huelga de profesionales

Huelga Ordinaria Industrial
Establecimiento de huelgas
Huelga Industrial
Huelgas simpatizantes

Huelgas Restringidas
Huelga detalladas

Parachoques huelgas
Desaceleración de la huelga
Trabajo para descartar la huelga
Informes "enfermo" (paro por enfermedad)
Huelga por renuncia
Huelga Limitada
Huelga selectiva

Huelga Multi-Industrial
Huelga Generalizada
Huelga general

Combinación de Huelgas y Cierres Económicos
Hartal
Apagado Económico

Los métodos de no cooperación política

El rechazo de la autoridad
Suspensión o retirada de la lealtad
La denegación de las ayudas públicas
Literatura y discursos abogando por la resistencia

Ciudadanos sin cooperación con el Gobierno
Boicot de los órganos legislativos
Boicot de las elecciones
Boicot del Gobierno y las oposiciones

Boicot de los departamentos de gobierno, organismos y otros órganos
La retirada del Gobierno de las instituciones educativas
Boicot de las organizaciones apoyadas por el gobierno
La denegación de asistencia a los agentes del orden
La eliminación de letreros de propaganda y señales
La negativa a aceptar a los funcionarios nombrados
La negativa a disolver a las instituciones existentes

La acción gubernamental nacional
Evasiones casi-legales y demoras
No cooperación de las unidades gubernamentales constituyentes

Alternativas de los Ciudadanos a la Obediencia
Cumplimiento renuente y lento
No obedecer en ausencia de supervisión directa
No obediencia Popular
Disfrazado de desobediencia
La negativa de una asamblea o reunión para dispersar
Sentadas
No cooperación con el reclutamiento y la deportación
Ocultar, escapar, y falsas identidades
Desobediencia civil de leyes "ilegítimas"

Acción por el Personal de Gobierno
Denegación selectiva de la asistencia de colaboradores del gobierno
El bloqueo de las líneas de mando e información
Estancamiento y obstrucción
No cooperación con Administración General
Falta de cooperación judicial
Ineficiencia deliberada y no cooperación selectiva por agentes del orden
Motín

Acción Gubernamental Internacional
Los cambios en las representaciones diplomáticas y otros
Retraso y cancelación de eventos diplomáticos
Retener el reconocimiento diplomático
Ruptura de relaciones diplomáticas
Separación de las organizaciones internacionales
Rechazo de sus miembros en los organismos internacionales
Expulsión de organizaciones internacionales

Los métodos de intervención no violenta

Intervención Psicológica
Auto-exposición a los elementos
El ayuno
• Ayuno de presión moral
• Huelga de hambre
• Satyagraha rápido
Invertir juicio
Acoso No Violento

Política de intervención
La sobrecarga de los sistemas administrativos
Revelar las identidades de los agentes secretos
Buscar el encarcelamiento
Desobediencia civil de leyes "neutrales"
El trabajo en colaboración, sin soberanía dual y gobierno paralelo

Intervención Económica
Huelga Invertida
Mantenimiento de la huelga
Tomar las tierras sin violencia
Desafío a los bloqueos
por motivos políticos contra la falsificación
Compra excluyente
La incautación de activos
Volcado
Clientela selectiva
Mercados alternativos
Sistemas alternativos de transporte
Alternativas a las instituciones económicas
Obstrucción no violenta
Ocupación no violenta

Intervención Física
Sentarse en
Estar en
Pasear en
Caminar en
Batir en
Orar en
Ataques No violentos
Ataques aéreos No violentos
Invasión No violenta
Interjección No violenta

Intervención Social
El establecimiento de nuevos patrones sociales
La sobrecarga de las instalaciones
Puestos en
Hablar en
Guerrilla teatro
Alternativa instituciones sociales
Sistema alternativo de comunicación

Guía sobre seguridad en enfrentamientos callejeros

(compilado a partir de http://www.dailykos.com/story/2011/2/3/941050/-Guide-to-Safety-and-Victory-in-Street-Confrontations-UPDATE

Los siguientes consejos son proporcionados por los veteranos de batallas callejeras en diversos contextos. Todo el que busca usarlos debe tratar de llevar la mayor cantidad de los materiales descritos como sea posible a fin de proporcionar extras para otros. Pero no llevan demasiado, ya que hará más difícil moverse rápidamente cuando sea necesario.
Recuerde: Para grabar y documentar, y que pueda verlo el mundo, y actuar, llevar más de un dispositivo de grabación y mantener uno oculto, si es posible, y de tal manera que usted puede configurarlo para grabar sin que sea descubierto.

Recuerde, la capacidad de carga del grupo también cuenta. Distribución de suministros según su grupo de estrategia y hacerlo del modo más equitativo posible entre los manifestantes.

Protección y Seguridad

Cabeza

Los cascos de bicicletas ofrecen una buena protección. En los diseñados para las carreras no cuesta trabajo tener toda la cara cubierta y son los más seguros. Cascos de construcción también ayudarán a proteger la cabeza, y son tan ampliamente disponibles como los cascos de bicicleta.
Una toalla o un paño grueso envuelta alrededor de la cabeza puede proporcionar cierta protección, pero no es óptima. Se puede cubrir con un recipiente de metal o una olla para obtener más protección, pero es importante que se sea capaz de ver.
Recuerde: Un impacto fuerte en la cabeza todavía puede causar lesiones internas, aunque el exterior de la cabeza parece ileso. No lleve cosas que fácilmente puedan ser arrancadas (como colgantes pendientes y otras joyas).

Cara

Máscaras hacen difícil identificar a los individuos, y si todo el mundo lleva máscaras nadie destaca.
Las capuchas cubrirán la mayor parte de sus caras y las gorras de béisbol ayudan a protegerse de la mayoría de cámaras montadas en las calles. Algunas de las mejores máscaras son las camisetas. Ponga su cabeza en una camisa, use el agujero para el cuello agujeros para los ojos y atar las mangas alrededor de la parte posterior de la cabeza.
La mejor protección contra las armas químicas es una máscara de gas. Cualquier tipo de máscara debe ser revisada comprobando que es de su tamaño antes de que esté en las calles y se sea difícil encontrarlas. Cuando se combinan con las gafas, las mascarillas son una excelente alternativa a las máscaras de gas. Es necesaria una cierta preparación de antemano, y encontrar gafas que sean irrompibles y que no se empañen, y que se ajusten bien en su cara con el respirador o la mascarilla. Los respiradores o mascarillas pueden estar disponibles en tiendas de seguridad o en los vendedores de artículos de soldadura. Solicite filtros para partículas y sustancias químicas orgánicas y dígale al secretario lo que está filtrado para corroborar.
Un pañuelo empapado en agua o vinagre y atado fuertemente alrededor de la nariz y la boca es un último recurso. Es mucho mejor que nada, pero recuerda que no es más que un obstáculo y no un filtro y que no será muy efectivo para la protección a largo plazo. Usted puede mantenerlo en remojo en una bolsa de plástico hasta que esté listo para usarlo. Lleve varios, para usarlos a la vez, el uso de un solo pañuelo frente al gas, es como respirar el aire que te rodea. Para la protección de los ojos, las gafas de natación funcionan bien ya que tienen un sello hermético. Destruir la resistencia es muy importante (una bala de goma en el ojo puede ser desastroso). La mayoría de gafas tienen agujeros de aire para prevenir el empañamiento puedes rellenarlos con epoxi. Cubriendo estos agujeros con cinta adhesiva puedes salir de un apuro frente a un ataque inicial, aunque no valen para la protección a largo plazo. Pruebeselos combinados con su respirador, mascarilla o pañuelo para garantizar que sean compatibles y que ambos proporcionan un sello hermético. No use lentes de contacto, pueden atrapar sustancias químicas irritantes debajo.

Ropa

Use ropa gruesa eso le servirá de muralla para los objetos que sean lanzados. Múltiples capas puede ayudar a proteger contra fracturas de huesos u otras lesiones graves. Use guantes de trabajo pesado si piensa para manejar

botes calientes de gas lacrimógeno. Ropa limpia en una bolsa plástica (pueden contaminarse por las armas químicas)

Calzado

Este debe ser relativamente resistente, pero aún así cómodo para moverse, y no resbaladizos, y si es posible, resistente a productos químicos. No use nada que pueda patinar, haga lazos para atar los cordones de doble nudo, etc.

Piel

Evite el uso de vaselina, aceite mineral, protector solar con base en aceite, lociones, cremas hidratantes, o detergentes en la piel porque estos pueden atrapar los químicos y por ende prolongar la exposición. Lave su ropa, cabello y piel de antemano con jabón libre de detergentes. Recomendamos utilizar protector solar a base de agua o alcohol (en lugar de a base de aceite). Si su elección está entre base de aceite o nada, te recomendamos usar el protector. Recibir un rocío de pimienta encima de una quemadura por el sol no es nada divertido. También es recomendable minimizar la exposición de la piel cubriéndola lo más que se pueda.

Brazos

Use algo para proteger los antebrazos, ya que estos son una cobertura natural para la cara/cabeza. Unas canilleras o papel periódico enrollado son buenas alternativas. El hule espuma es práctico y muy ligero para ser usado como protección contra cualquier clase de golpe. Las sillas y escaleras plegables también sirven como protección personal.

Suministros

Tenga a la mano agua y frazadas para ser usadas en caso de que una persona se prenda fuego. Use la frazada mojada para apagar el fuego. No intente usar agua para apagar fuegos iniciados con petróleo (gasolina). Incluso un simple kit de primeros auxilios puede ser muy útil en circunstancias (ver más adelante).

Seguridad en Números

Permanezca alerta y consciente de su seguridad y la de las personas que lo rodean.
Recuerde siempre evitar la violencia tanto como se pueda para proteger la legitimidad de la causa.

Comida

Evite el alto consumo de proteínas durante el tiempo de actividad ya que esta es difícil de digerir y le hará más lento.
Los carbohidratos son buenos para mantener el cuerpo energizado. Consuma bananas, también son buenas. El azúcar es un remedio rápido en situaciones de falta de energía, pero puede causar que su nivel de azúcar en la sangre disminuya rápidamente más tarde.
Cuídese bebiendo lo suficiente. En tiempo de inactividad, cuando tenga algunas horas para descansar, intente si puede, tener una comida balanceada y saludable, también descansar un poco.

Lista de objetos necesarios para ayudar a los manifestantes:

- Toallas
- Agua
- Extintores de incendios (no se lleve todos los extintores de un área, solo los que sobren)
- Frazadas y frazadas contra fuego si es posible
- Cascos de construcción, de bicicleta, y cualquier otra protección para la cabeza, equipos de protección deportiva, protección para motociclistas, y equipo todo terreno
- Vasijas y ollas de metal que puedan actuar como protección para la cabeza en combinación con toallas o cualquier otro relleno interior
- Ropa gruesa
- Kit de primeros auxilios
- Escalera plegable
- Escaleras plegables y otros instrumentos que puedan ser usados como escudos
- Jabón y desinfectantes
- Ganchos (imperdibles) y cinta pegante

Algunos objetos recomendados para el kit de primeros auxilios

- Cinta pegante
- Alcohol
- Toallitas húmedas
- Analgésicos
- Hisopos.
- Guantes desechables de látex.
- Vendajes elásticos.
- Mascarilla para RCP
- Linterna
- Botella con agua caliente
- Agua oxigenada (peróxido de hidrógeno)
- Ganchos (imperdibles)
- Sal
- Tijeras
- Azúcar o solución con glucosa
- Termómetro
- Cinta a prueba de agua

Puede revisar el "Guide to Protecting the North African Revolution" para información adicional sobre defensa, ofensiva, tácticas y seguridad. La puede encontrar en Google.

Gas Lacrimógeno

Si se espera recibirlo:

- Si lo ve venir o le llega una advertencia, póngase el equipo de protección.
- Si es posible, trate de alejarse o ponerse en contra del viento.
- Mantenga la calma, el pánico incrementa la irritación.
- Respire lentamente y recuerde que el efecto es temporal.
- Suénese la nariz, enjuague la boca, tosa y escupa. Intente no tragar saliva.
- Si usa lentes de contacto, intente quitarlos o pida a alguien que se los quite, con los dedos limpios.

Si se expone al gas:

Para los ojos:
Recomendamos una solución de ½ parte de antiácido líquido (leche de magnesio) y ½ parte de agua. Una botella de spray sería lo ideal para esto, pero una botella con tapa de chorro funciona igual de bien. Siempre humedezca de las esquinas interiores del ojo a las exteriores, con la cabeza hacia atrás y ligeramente ladeada hacia el lado que se está enjuagando. Desde nuestra experiencia parece ser que es necesario que la solución caiga directamente en los ojos para que funcione. Esto significa que si la persona afectada dice que está bien, debería intentar abrir sus ojos por ella y aplicar la solución. En la mayoría de los casos las personas afectadas no podrán abrir los ojos por ellos mismos, el abrirlos incrementara el dolor temporalmente, pero la solución acuosa ayudará. También funciona espectacularmente como enjuague bucal.

Para la piel:
Recomendamos aceite de canola, seguido de alcohol. Evite que caiga en los ojos, frote cuidadosa la piel que fue expuesta al químico, frote cuidadosamente la piel expuesta con un trapo o una gaza saturada con aceite de canola. Después de esto aplique inmediatamente alcohol y frote. Recuerde que el alcohol en los ojos lastima Y MUCHO. Cualquier persona cuyos ojos hayan sido lastimados con alcohol por su culpa, dejará de ser su amigo.

El tratamiento secundario puede incluir:
Escupir, soplarse la nariz, toser toda la mucosa (No quiere tragarse todos esos químicos!). Caminar con los brazos extendidos, quitándose toda la ropa contaminada, y tomar una ducha fría. De hecho, es esencial tomar una ducha y lavar la ropa (esta vez con detergentes) tan pronto como se pueda. Este agente es bastante tóxico y continuamente le contaminara y a todos los que le rodean hasta que se deshaga de él. Mientras tanto, intente no tocarse la cara ni los ojos o a otra gente o muebles, alfombras etc. para evitar mayor contaminación. Recuerde, es solamente temporal y nosotros somos extremadamente fuertes.

Mantenerse a salvo y sensible en acción

Una manifestación donde la policía puede atacar requiere más altos niveles de conciencia táctica que una manifestación promedio. Aquí encontrará algunas sugerencias aplicables que pueden ayudar a mantenerse seguro y efectivo en las calles.

Siempre tenga un lugar seguro en mente. Todos los manifestantes necesitan tener en cuenta un lugar seguro para ir si la situación se sale de las manos. Defina lo que es “seguro” e “inseguro” por usted mismo. Para algunos, la seguridad está entre los brazos de los compañeros activistas, justo en la línea frontal, pero no hay nada de vergüenza en tener un refugio a donde ir, por un sinnúmero de razones. Los lugares seguros cambian dependiendo del movimiento y de las barreras impuestas por otros manifestantes y la policía. En algunos casos se incluyen lugares con espacios abiertos y áreas públicas. En otras ocasiones pueden tomar la forma de un callejón u otro lugar similar. No hay regla alguna acerca de encontrar un lugar seguro, pero se debe tener en mente un lugar antes de que empiece a volar mierda por todos lados.

Siempre tenga una salida en la mente, evalué la manera de salir de una mala situación. Tal vez lo mejor sea estar junto a un grupo grande por protección. Pero si la policía te arrea como el ganado, entonces el grupo grande será su objetivo y probablemente tendrá que separarse y huir en grupos más pequeños. Escapar en algunos momentos tal

vez sea la única oportunidad que se tenga para estar activo la próxima vez. Organice con sus amigos como salir del lugar y como reagruparse si son separados.

Use el sistema de amigos y muévase en grupo. Si es posible, asegúrese de tener un compañero en quien confiar, con quien siempre se mantendrá cerca. De esa manera, por lo menos una persona sabrá donde se encuentra y cuál es tu condición. Trabajar en grupos pequeños de personas con quienes conoce bien y a quienes confiaría su propia seguridad también es otro factor importante. Incluso si no se es parte de un grupo organizado con un plan de acción, ayuda mucho estar con amigos en quienes se pueda confiar.

Tenga en cuenta las dinámicas de la multitud y sus peligros. Es necesario que sepa qué está ocurriendo, no solo a su alrededor sino en las esquinas siguientes y unas cuadras más adelante. Preste atención al estado de ánimo de la multitud y el de la policía. Ciertas acciones como destrucción de la propiedad privada y violencia serán probablemente ocasionadas por o como resultado de un comportamiento violento por parte de la policía. Tenga en cuenta el movimiento de la policía y el de diferentes grupos de manifestantes entrando o saliendo de un área. Intente monitorear los sentimientos y objetivos de los amigos y enemigos en todo momento.

Entérese de lo que está ocurriendo fuera de la vista al enviar exploradores para que investiguen lo que la policía y otros manifestantes están haciendo ya que la situación en una protesta dinámica cambiará frecuentemente y de manera rápida. Los exploradores necesitan revisar y enviar un reporte muy seguido, es una buena idea el apuntar algunos miembros del grupo como exploradores.

No actúe por rumores. Es común en las manifestaciones que alguien se acerque a un grupo de activistas y empiece a gritar: “La policía Antidisturbios viene!” tan común como puede ser que ni siquiera hay policía en camino. Esta gente puede estar en pánico, o pueden ser agentes sin uniforme tratando de confundirte. Actuar bajo mala información es perjudicial, y mayormente peligroso. Toda la información crítica necesita ser verificada. Si la persona que da la información no puede afirmar que presenció en persona los hechos, o él/ella es un extraño, entonces esta información no es de confiar.

Asuma que los policías antidisturbios pueden estar llegando. Mientras que actuar bajo rumores y ser alarmista puede ser disruptivo y peligroso, no debería sorprender cuando las “autoridades” decidan cuando bloquear, rodear, irrumpir y disipar una manifestación. Esto ocurre con frecuencia, y la clave para no ser atrapado es mantenerse preparado.

Que no cunda el pánico; ayuda a otros a mantenerse calmados, A veces en las acciones, la situación puede volverse aterradora. Pero el pánico reduce el juicio crítico, la manera de adaptarse y la habilidad de afrontar la situación y, además, puede dispersarse rápidamente. Nuestra mejor defensa es la calma colectiva, manteniéndonos los unos a los otros centrados y enfocados. Si no puede mantenerse centrado y enfocado, entonces necesita dejar la demostración para calmarse. Similarmente, si alguien más no puede mantener la calma, necesita irse.

La mejor ofensa y defensa es hacer parte de un grupo sólido. Los grupos combinan varias habilidades y poderes. Los grupos sabios practican seguido, planean, desarrollan estrategias y tácticas increíbles que van más allá de la habilidad de un individuo. Tienen la cantidad de gente necesaria para hacer varias tareas: actuar, explorar, servicio médico, comunicarse con los demás, seguridad, etc., sin embargo, son lo suficientemente pequeños para actuar rápido.

Luchando contra las Tácticas Policiales

Comúnmente, la estrategia policial en una protesta que quieren terminar es dispersar a sus participantes. Ellos tienden a operar en unidades coordinadas, y usan las siguientes tácticas:

- Demostraciones de fuerza para intimidar y asustar a la gente para que se vayan.
- Ataques sorpresa por tropas ocultas en reserva.
- Rodear y aislar una multitud entera – algunas veces sin permitir a la gente entrar o salir. También podrían intentar dividir la multitud abalanzándose sobre ella en su punto más débil. Si ve que la policía está a punto de atacar su punto más débil, intente reforzarlo. Cuando los manifestantes se están dispersando, ellos intentarán conducirlos como ganado hacia ciertas áreas, y lejos de otras. Se puede evitar esta maniobra

dividiéndose del grupo. Esto puede ser efectivo, si la policía está operando con unidades pequeñas y no se está dispersando para tratar con grupos pequeños fuera de la multitud.

- A menudo la policía usará escuadrones de captura para hacer arrestos sorpresa de individuos que han elegido al azar entre la multitud o de quienes ellos han identificado como “líderes” o “revoltosos”. Los escuadrones de captura comúnmente se componen o colaboran con agentes encubiertos y pueden atacar en cualquier momento. El mejor momento para evitar una captura es justo en el instante en el que esta ocurrió. Se necesita un grupo de gente que rompa la barrera policial, y otro grupo que actué como barricada. Un rol importante y de bajo riesgo en suprimir estos arrestos involucra simplemente el ubicarse entre la policía y su objetivo. Una vez la persona sea rescatada, todos deberían soltar sus escudos y desaparecer entre la multitud. La policía puede intentar capturar uno de los rescatistas. Rodear los vehículos policiales que tienen a los capturados e impedir que se muevan, puede conducir a que las personas sean liberadas. Los autos no se mueven bien si tienen los neumáticos desinflados, pero ten en cuenta que cuando se pincha un neumático puede hacer mucho ruido.

Siempre permanecer atento de dónde se encuentran los amigos, y permanecer preparado para actuar con claridad y sensatez en el momento de ser notificado.

Superar a la Policía:

No deje que lo intimiden hacia los andenes o aceras. La policía presionará a las marchas a los andenes o aceras para estrechar la multitud y dividirla en grupos más pequeños. Una vez la policía ha forzado una marcha a los andenes o aceras , pueden dirigir sus movimientos más fácilmente e individualizar a los revoltosos.

Los cruces pueden ser usados para moverse de nuevo hacia la calle. En casos en los que se encuentre gente y personas en bicicleta, estas pueden ayudar a formar barreras, las cuales ralentizarán a la policía que intenta presionar la marcha.

La policía se mueve lento, así que muévete rápido en un grupo grande y apretado. Ocasionalmente correr de manera ordenada, ayudará a mantener siempre a la policía detrás del grupo. Hacer una cuenta regresiva no solamente intimidará a la policía, sino que llenará a la gente de vigor cuando empiecen a correr. Moverse en contravía por un carril de una sola vía puede estrechar a la manifestación (ya que las personas deben hacer espacio para los autos detenidos), sin embargo se hace muy difícil para grupos grandes de policía el seguirla. Mire por fuera de la multitud, si a alguien se le está administrando primeros auxilios, alejarse de el para que no se presenten inconvenientes.

Formar cordones rodeando lo que la policía quiere (edificios, equipos de sonido, etc.). Sentarse en el suelo es bueno para disuadir a la policía de atacar, pero solo si se está en grupos grandes. Algunas veces sentarse no vale la pena. Los caballos son impredecibles, particularmente los de policías violentos, especialmente quienes emplean munición de goma. Puede ser peligroso sentarse en frente de ellos.

Lanzar cosas es un acto defensivo. A veces no es sabio lanzar objetos todo el tiempo, eso solamente provocara a la policía y hará que desee golpear a la gente con más fuerza. Si se desea lanzar algo, hacerlo defensivamente, con estrategia y en masa. Una lluvia constante de escombros creará una “zona estéril” donde la policía no querrá ir. No lanzar jamás objetos para atacar o causar daño. Lánzalos desde el frente y luego desaparece con la multitud, solo los idiotas lanzan cosas desde la parte de atrás.

Las latas de gas pueden ser lanzadas o pateadas fuera de la multitud antes de que exploten. Hay que ser cuidadoso, y no cogerlas con las manos desnudas, ya que pueden estar muy calientes. Y explotarán.

Las barricadas pueden ser más problemáticas de lo que parecen. Un taponamiento impasable puede ser inconveniente cuando se necesita correr. Las mejores barricadas son materiales al azar como cajas de periódicos, contenedores de basura volteados o material para construcción, esparcido por el lugar. Uno o dos grupos de personas pueden usar la fuerza colectiva para levantar vehículos pequeños que estén aparcados y ubicarlos en medio de la calle sin dañarlos.

La mejor defensa es el caos, si la situación cambia constantemente la policía no puede seguir el paso. Hay que cambiar de apariencia, abrir nuevas direcciones y posibilidades, ser impredecible.

Hay que tener cuidado con los provocadores, incluyendo pero no limitado a “policía de paz”. Estos autoproclamados funcionarios de “paz” se infiltran en las manifestaciones e intentan impedir que la gente camine por la calle o se involucre en alguna forma de protesta. Algunas veces usan brazaletes (comúnmente blancos) e intentan reportar gente a la policía o arrestarla personalmente. También hay que tener cuidado con personas que instiguen a la violencia contra lugares u objetos que no son un objetivo obvio. Esta gente es comúnmente empleada por la policía para desacreditar la manifestación.

Enfrentando a la Policía:

En cualquier multitud ruidosa, habrá policía intentando dispersarla. Ellos tratarán de dispersarla embistiendo con bastones, caballos, vehículos, gas lacrimógeno, munición de goma o madera y unos cuantos arrestos violentos.

Los pasos de baile de la policía incluirán una o más de estas opciones:

- Rodear a la multitud con policías en fila.
- Desde el centro o desde los lados, la formación policial forzará a todos hacia los andenes o aceras tratando de filtrar los “espectadores” de los “actores” en la multitud.
- Ataques con Bastón/Caballo/Gas para disminuir la moral.
- Sonido a alto volumen, y granadas de conmoción, para desorientar y separar a la multitud.
- Las cargas en línea empujarán lentamente a la multitud en la calle hacia donde ellos quieren (carga, retroceso, reorganización, carga, retroceso, etc.)
- La policía no puede arrestar grandes grupos de gente a menos que tengan muchas tiras plásticas para utilizar como esposas.
- La policía no utilizará gases lacrimógenos a menos que tengan puestas sus propias máscaras

Evite que se formen las líneas! Rodearlo y prevenir que usted se desplace como lo desee y empujarlo en la calle hacia donde ellos desean requiere que la policía tenga una fila muy fuerte. Es importante prevenir que las primeras líneas se formen. Si la multitud parece ser volátil ellos retrocederán y se reorganizarán más atrás pero si la multitud está distraida o confundida y pasiva ellos tratarán de mezclarse y formar sus líneas dentro de la multitud.

- No se quede parado mirándolos. Manténgase en movimiento
- No de la impresión de que va a permitir que ellos se le acerquen.
- Busque brechas entre la multitud y rellénelas. Manténgase juntos y unidos.
- Trate de adelantarse a sus movimientos y llegue allí antes.
- Proteja las rutas de escape parándose frente a ellas.
- Movilice a quienes se volvieron "espectadores" de nuevo hacia la multitud y muévase entre ellos.

Ellos podrán empezar a cargar y a arrestar. Usted estará en un posición muy fuerte y con sus rutas de escape aseguradas. Lo que sea que ocurra después, no lo espere parado allí, manténgase en movimiento y actúe de manera defensiva.

Si bloquearon su única salida, trate de avanzar en contra:

- esto requiere que usted avance su líneas contra las de ellos, ganando más espacio y abriendo más salidas.
- utilice la línea frontal como un muro sólido, enganchando los brazos y moviéndose lentamente hacia adelante.
- haga una cuenta regresiva para forzar un avance más rápido.
- utilice cualquier pancarta como escudo (prevendrá que rompan su línea). Los contenedores de basura, caballetes, cercas o barandas también son útiles.

Si bloquearon la única salida, reorganícese.
Siempre busque opciones para aumentar de tamaño el grupo, de unirse con otros grupos y absorber a los rezagados. Todos tendrán que salir de allí y usted tendrá una mejor oportunidad de salir sano, con todas sus pertenencias y equipo si se van todos juntos al mismo tiempo.

FAQs (En ningún orden particular.)

P: Pueden ayudarme?
R: Revise http://anonhispano.blogspot.com/ o únase a irc.iranserv.com, en un canal como #iberoamerica o contacte a algún operador. Otra opción es contactar a Anonymous en Twitter o Facebook.

P: Tienen algún sitio web?
R: http://anonhispano.blogspot.com/

P: Cómo sé lo último en noticias?
R: Esté pendiente de los canales de IRC o visite http://www.anonnews.org y http://anonhispano.blogspot.com/

P: Las noticias de AnonNews o AnonHispano son oficiales?
R: Bueno, en cierta manera son oficiales. Por un lado son "oficiales" y por otro, a mayor número de personas que apoyan una operación, más oficial se vuelve.

P: Porque no atacar periódicos/ televisión/ estaciones de radio?
R: Anonynmous no ataca a los medios de comunicación.

P: Esos no son medios de comunicación. Solo riegan mentiras y propaganda (política…puede ser). Todos están manipulados por el gobierno.
R: La libertad de expresión también es válida para los imbéciles.

P: Pero, pero…..
R: Como Evelyn Beatrice Hall dijo : "Estoy en desacuerdo con lo que dices, pero defendería hasta la muerte tu derecho a decirlo".

En las palabras de Noam Chomsky: "O crees en la libertad de expresión, precisamente porque hay puntos de vista con los que no estás de acuerdo, o no crees en la libertad de expresión".
Libertad de expresión, entendido?

P: WTF? Entonces hay reglas?
R: Si, no ataques a los medios y no incentives la violencia. Sencillo, verdad?

P: Para qué son buenos los DDoS y los defacements? No ayudan a la gente.
R: Los DDoS tienen como finalidad llamar la atención de los medios hacia los problemas de la gente. Si los medios se dan cuenta y publican la noticia, esto ayuda a la gente. El fino arte de mutilar un sitio web busca enviar un mensaje a la gente y al propietario de ese sitio. Además, Anonymous provee a la gente de información, guías y software para evitar la censura (también conocido como el Paquete de Protección)

P: Qué es el Paquete de Protección?
R: Software como Tor Onion Router, un manual o guía para evitar la censura, más software, otras guías y más cosas útiles.

P: Me podrían suministrar una guía para desarrollar botnets?
R: Esa guía no existe.

P: He visto este link para una descarga en el canal, puedo confiar en el?
R: Anonymous recomienda no confiar en links que aparezcan en los canales. Los únicos que pueden ser confiables son aquellos que ponen los administradores, operadores y los que se encuentren en el asunto del canal.

P: Alguna persona en IRC me preguntó en dónde vivo y cuál es mi nombre.
R: NUNCA provea información personal en IRC. Contacte inmediatamente a un operador o Administrador y coméntele lo que ocurrió. También lo deberá hacer con cualquier comportamiento sospechoso.

P: Cómo puedo unirme a su club?
R: Anonymous no es un club.

P: Qué es Anonymous?
R: Anonymous es un movimiento general. No es un grupo con miembros fijos u objetivos rígidos. Es un movimiento fluido del que cualquiera puede hacer parte, simplemente participando. Para ser parte de Anonymous lo único que tiene que hacer es acompañarnos en cualquiera de nuestras actividades.

P: Pero, cómo es que funciona esta cuestión de Anonymous?
R: La mejor forma de saberlo es entrando a un canal, estar pendiente y formar una idea. Cualquiera que crea que la libertad de expresión es una meta remunerativa puede volar con una bandera de Anonymous.

P: No soy un hacker, cómo puedo ayudar?
R:

- recopilando y difundiendo información
- organizando
- haciendo contactos
- dando sus puntos de vista
- compartiendo experiencias
- oprimiendo el botón de IMMA FIRING MA LAZOR
- escribiendo guías
- traduciendo
- ...

P: Existe un Hive?
R: 1. N00b, mire en el asunto del canal digitando /topic
2. Probablemente no pero no es necesario un hive, puede disparar manualmente si lo desea.

P: De dónde puedo descargar el LOIC?
R: N00b, mire en el asunto del canal digitando /topic
O, directamente en https://github.com/NewEraCracker/LOIC/downloads

P: Cuál es el objetivo?
R: N00b, mire en el asunto del canal digitando /topic

P: El objetivo está caido?
R: Visite www.watchmouse.com y verifíquelo ahí.

P: Algunos usuarios me dicen que había unas chicas danesas en #canal.
R: Obviamente se trata de una mentira, no hay chicas en Internet.

P: Qué es un netsplit?
R: Un netsplit es la demostración de las teorías evolucionistas de Darwin en Internet.

P: Por qué no puedo entrar a la red IRC de Anonymous con Tor?
R: Porque por culpa de algunos vándalos (no estoy mirando a nadie) Tor ya no está permitido en los canales IRC de Anonymous. Puede utilizar I2P. Para recibir ayuda pregúntele a un bot llamado "muninn". Muninn es el bot que la gente de I2P utiliza para conectarse a la red IRC de Anonymous.

P: Soy un chico de los medios, cómo puedo contactarlos?
R: Visite http://anonhispano.blogspot.com/

P: Soy una chica de los medios, cómo puedo contactarlos?
R: Visite http://anonhispano.blogspot.com/

P: Ok, soy de los medios y necesito hablar con el representante/líder/estratega de Anonymous.
R: Anonymous no tiene líder ni representante ni estratega.

Algunos links

Trabajo colaborativo:

- http://piratepad.net
- http://www.typewith.me
- http://www.piratenpad.de

Polls:

- http://pollcode.com

Pastebins:

- http://pastebin.com
- http://pastebin.de
- https://www.pastee.org

Puedes cifrar tu material, hay que subir un certificado SSL:

- http://tinypaste.com

Informacion acerca de sitios web:

- http://www.robtex.com
- http://news.netcraft.com

Email desechable:
Utilice estos para registrar actividades en su cuentas de email/facebook/twitter

- http://10minutemail.com

- http://www.sofort-mail.de
- http://www.trash-mail.com
- http://www.guerrillamail.com
- http://www.spam.la

Software Portable:
Software Portable es software que se puede ejecutar desde un memoria USB para no dejar rastros en su computador

- http://portableapps.com
- http://portableapps.com/apps/internet/firefox_portable
- http://portable-i2p.blogspot.com

Proxies:
Pueden ser usados en conjunto con una VPN.

- http://www.freeproxies.org
- http://www.socks24.org
- http://www.samair.ru/proxy

VPN

Gratuitas:

- http://cyberghostvpn.com
- http://hotspotshield.com ocasionalmente revisa el trafico y lo redirige a anunciadores.
- http://proxpn.com
- https://anonymityonline.org
- http://www.bestfreevpn.com
- http://www.your-freedom.net

- http://www.ultravpn.fr
- http://www.itshidden.com
- http://www.thefreevpn.com
- http://www.packetix.net

De pago pero más seguras:

- http://www.swissvpn.net
- http://perfect-privacy.com
- https://www.ipredator.se
- http://www.anonine.se
- https://www.vpntunnel.se
- http://www.relakks.com
- http://www.steganos.com
- http://www.bananavpn.net registra IPs
- http://www.strongvpn.com registra IPs
- http://www.secureix.com
- http://www.secretsline.com

I2P

- http://geti2p.net

Chat para mas informacion de I2P:

- https://www.awxcnx.de/i2p-irc-en.htm

Tor Onion Router:

- http://www.torproject.org

Privacy Box (La caja privada):
Privacy Box proporciona formas de contacto no rastreables (y algo anónimas). Opera sobre todo para los periodistas, bloggers y otros editores pero está abierto para otra gente también. Pensamos en correos electrónicos

- https://privacybox.de/index.en.html

Envió de coreos anónimos:

- https://www.awxcnx.de/mm-anon-email.htm

Servidores DNS gratuitos y sin censura:

- 87.118.100.175 (Puertos: 53, 110)
- 94.75.228.29 (Puertos: 53, 110, HTTPS-DNS, DNSSEC)
- 62.75.219.7 (Puertos: 53, 110, HTTPS-DNS, DNSSEC)
- 87.118.104.203 (Puertos: 53, 110, DNSSEC)
- 62.141.58.13 (Puertos: 53, 110, HTTPS-DNS, DNSSEC)
- 87.118.109.2 (Puertos: 53, 110, DNSSEC)
- 85.214.73.63 (anonymisierungsdienst.foebud.org)
- 204.152.184.76 (f.6to4-servers.net, ISC, USA)
- 2001:4f8:0:2::14 (f.6to4-servers.net, IPv6, ISC)
- 194.150.168.168 (dns.as250.net; anycast DNS!)
- 213.73.91.35 (dnscache.berlin.ccc.de)
- 80.237.196.2
- 194.95.202.198

Para saber si usted lo está utilizando apropiadamente, abra su navegador y escriba http://welcome.gpf en de la barra de direcciones, si le aparece el siguiente mensaje "Congratulation You are using a censorship free DNS server!“. Está bién.

Si usted es un hax0rz puede usar la terminal, abra una y escriba nslookup welcome.gpf
Non-authoritative answer:
Name: welcome.gpf
Address: 62.75.217.76
De otra forma, falló.

Enviar faxes gratis:

- http://sendfreefax.net (Texto solamente)
- http://www.freefax.com/ff_snd.html (Texto solamente)
- http://www.eztel.com/freefax/ (Texto solamente)
- http://www.popfax.com Capacidad para pdf, 2 faxes gratis al registrarse en la versión de prueba gratuita, no son necesarios tarjeta de credito / detalles de pago.

En protestas no violentas:

- http://www.aeinstein.org

Telecomix:
(...) Es un conjunto descentralizado de activistas de la red que han unido sus fuerzas para colaborar en las cuestiones relativas a el acceso a un Internet libre, sin vigilancia intrusiva.

- http://www.telecomix.org