CEBOLLIZA TU FLUJO DE TRABAJO

CON ONIONSHARE PUBLICA CONTENIDOS Y COMPARTE ARCHIVOS DE FORMA SEGURA

OnionShare es una herramienta de código abierto que te deja compartir archivos anónimamente y de forma segura, alojar sitios web, y hablar con amigues usando la red Tor.

`onionshare.org`

COMPARTE Y ACEPTA DOCUMENTOS DE FORMA SEGURA CON SECUREDROP

SecureDrop es un sistema de envío de documentos de informantes que organizaciones de periodistas y ONGs pueden instalar para aceptar documentos de forma segura desde fuentes anónimas.

`securedrop.org`

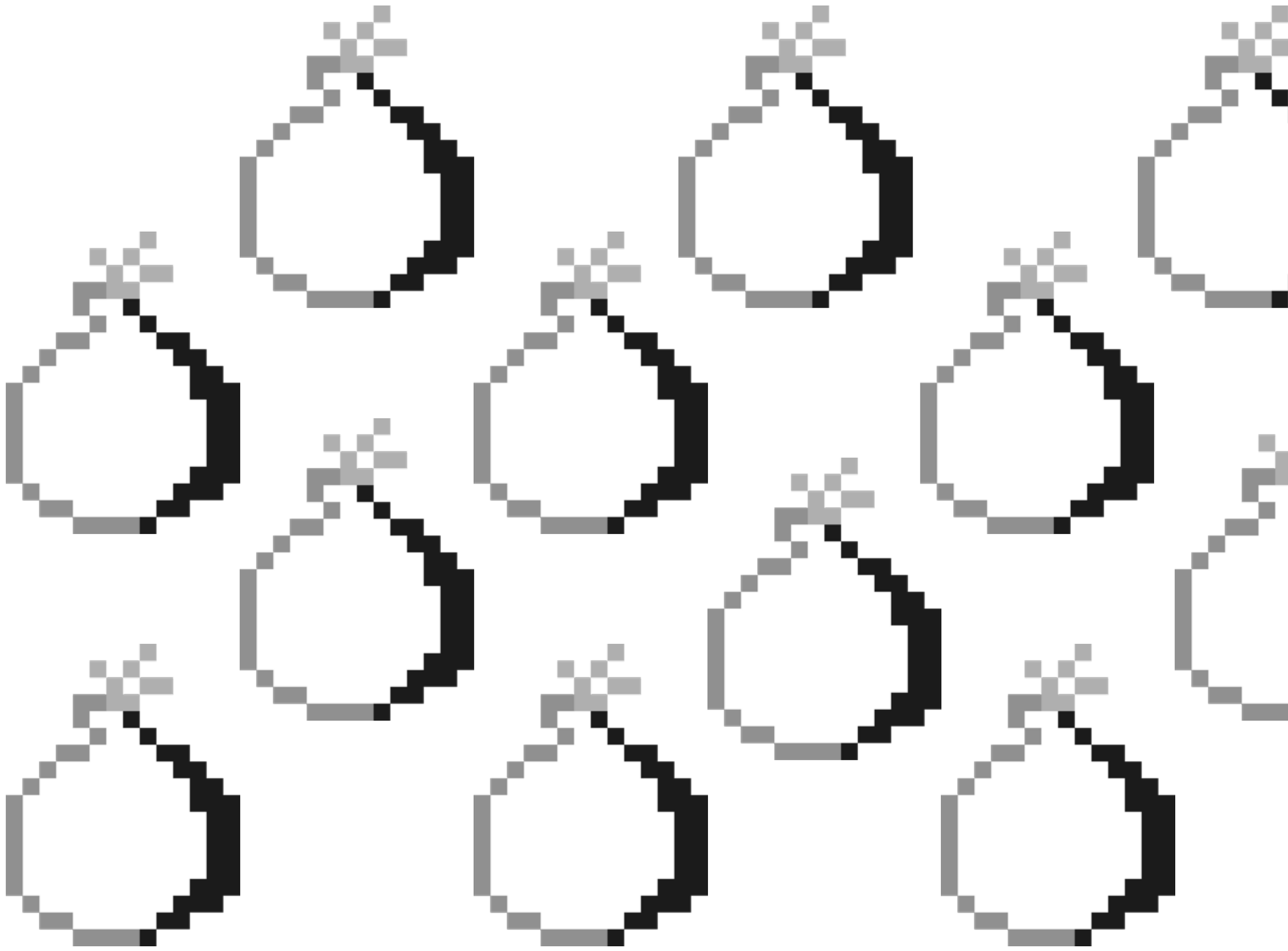
CON RICCOCHET PUEDES COMUNICARTE SIN METADATOS

Ricochet Refresh es una aplicación de mensajería de punto a punto que usa Tor para conectar clientes. Cuando inicias Ricochet Refresh, este crea un servicio onion Tor en tu computadora.

`ricochetrefresh.net`

`https://community.torproject.org/es-AR/onion-services/advanced/opsec/`

Cultiva tu cebolla



EL FUTURO ES CIBERFEMINISTA

Fernanda es parte de un colectivo de mujeres con foco en derechos reproductivos en Brasil, donde el aborto está criminalizado. Fernanda y sus colegas construyeron un sitio web con información de cómo acceder a un aborto, control de natalidad, y otros recursos para quienes estén buscando información sobre reproducción. Si este sitio web fuera conectado a ellas, podrían ser arrestadas o peor.

Por lo tanto Fernanda y sus colegas crearon el sitio web para que usara servicios onion de Tor, que no sólo las **protege de ser descubiertas como operadoras del servidor**, pero también ayuda a **proteger a sus visitantes** al sitio web al obligar a usar el navegador Tor.

CÓMO FUNCIONAN LOS SERVICIOS ONION?

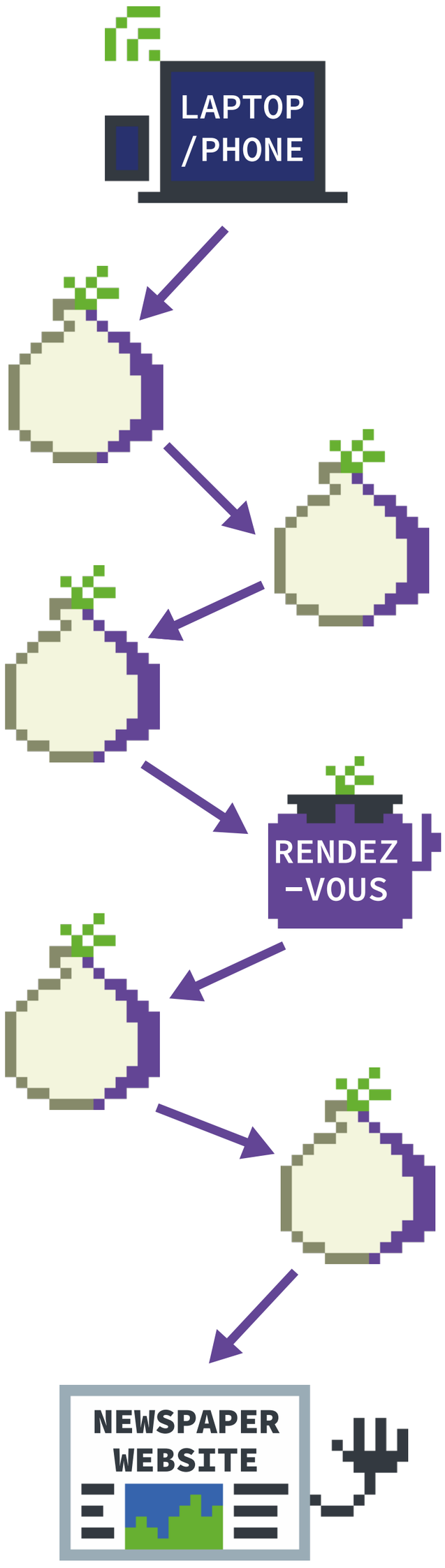
Los servicios Onion no se comportan igual que un relay en la red Tor. Un servicio Onion se conecta a los nodos rendezvous en la red tor; la coneccion de un cliente a un servicio onion hace lo mismo. Esto quiere decir que las conecciones del cliente al servidor nunca salen de la red Tor.

Un servicio Onion, al revés de mantener un relay Tor, no hace que tu dirección IP o servicio sean publicados en una lista pública en algun lado, ni tampoco tu servicio retransmite trafico de Tor.

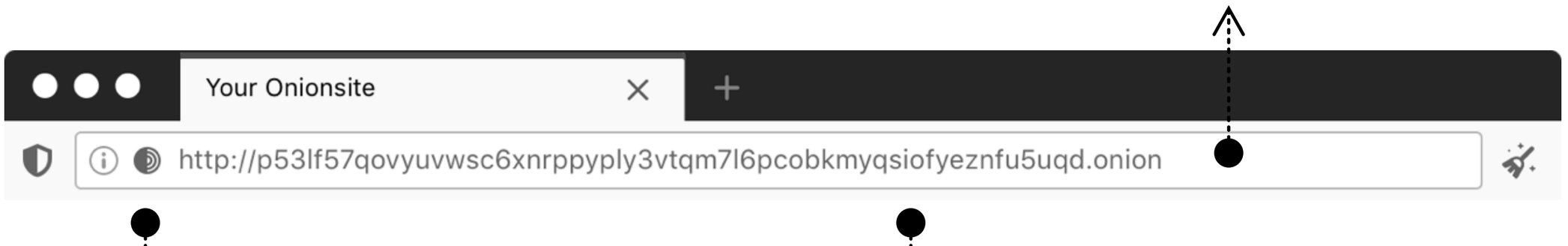
Desde el punto de vista de la red, el servicio onion se ve como cualquier otro cliente de Tor. Esto quiere decir que las operadoras de servicios onion no tienen que preocuparse de que el IP del servidor sea enlazado, marcada o puesta en una lista de bloqueo como parte de la red Tor.

Por más información sobre servicios onion, leer el portal de la comunidad del proyecto Tor:

https://community.torproject.org/es-AR/onion-services/overview/



IDENTIFICAR LA CEBOLLA



Icono de la cebolla

El pequeño icono de la cebolla que te ayuda a identificar los servicios Onion. Buscarlo en el navegador Tor.

.onion TLD

La dirección de un servicio onion es generada automáticamente, por lo tanto las operadoras no tienen que comprar un dominio; la URL .onion también ayuda a Tor asegurarse que estan conectados a la dirección correcta y que la coneccion no está siendo manipulada.

Direccion del Onion

Una dirección onion es una cadena de 56 caracteres (y 16 caracteres en el formato V2), mas que nada letras y números elegidos aleatoriamente seguido por un “.onion”. Todo el tráfico entre los servicios onion y usuarios Tor es encriptada de inicio a fin, por lo tanto no tienes que preocuparte de conectarte sobre HTTPS o no.

CULTIVA TU CEBOLLA

Cómo configurar un servicio onion para tu sitio web en un sistema operativo basado en Debian.

Nota: El simbolo # indica que se tiene que ejecutar ese código como root.

Tener un Tor funcionando

Seguir estas instrucciones para activar el repositorio de paquetes de Tor project:

1. Instalar apt-transport-https

Para poder activar todos los manejadores de paquetes usando la biblioteca libapt-pkg para acceder a metadatos y paquetes disponibles en fuentes accesibles sobre https (Hypertext Transfer Protocol Secure).

```
# apt install apt-transport-https
```

2. Agregar las siguientes lineas en el archivo /etc/apt/sources.list o en un nuevo archivo en /etc/apt/sources.list.d/

```
deb https://deb.torproject.org/torproject.org
buster main
deb-src https://deb.torproject.org/
torproject.org buster main
```

3. Ejecutar los siguientes comandos en la terminal para poder agregar la llave gpg usada para firmar los paquetes:

```
# wget -qO- https://deb.torproject.org/
torproject.org/
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc |
gpg --import
# gpg --export
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-
key add -
```

4. Instalar tor y el llavero de tor en debian

Ponemos a disposición el paquete de Debian para ayudarte a mantener actualizada nuestra llave de firmado. Es recomendable que la uses. Instalarla con los siguientes comandos:

```
 # apt update
 # apt install tor deb.torproject.org-keyring
```

Tener un servidor web que funcione

Nginx esta disponible en los repositorios principales de varias distribuciones Linux y *BSD. Para instalar el paquete `nginx`:

```
$ sudo apt install nginx
```

Por defecto, al final de la instalación, el servidor web estará funcionando en localhost:80.

Una vez que tu servidor web esta levantado, verifica que funciona: abre el navegador y visita a http://localhost/.

Ahora intenta colocar un archivo en el directorio html principal y verifica que se vea cuando accedes al sitio web en el navegador.

Configurar tu servicio onion

El siguiente paso es abrir el archivo de configuración de Tor (torrc) y hacer las configuraciones correctas para montar el servicio onion. Dependiendo de tu sistema operativo y configuración, el archivo de configuración de Tor va a estar en diferentes lugares o verse diferente.

Tienes que agregar las siguientes dos líneas a tu archivo `torrc`:

```
HiddenServiceDir /var/lib/tor/onion_service/
HiddenServicePort 80 127.0.0.1:80
```

Guarda el archivo torrc y reinicia Tor.

```
$ sudo systemctl restart tor
```

Si Tor se vuelve a iniciar, genial! Sino, algo no funciona. Primero busca en tus archivos log por alguna pista.

Editar el archivo de configuración del sitio web

Si estás corriendo varios sitios onion en el mismo servidor web, recuerda editar el archivo virtual host del servidor web y agregar la dirección onion a cada sitio web.

Chequear que tu servicio onion funcione

Para conseguir tu direccion del servicio onion, ve al directorio `HiddenServiceDir`, y busca un archivo llamado `hostname`. El archivo `hostname` en tu directorio de configuración del servicio onion contiene el hostname de tu nuevo servicio onion v3. Los otros archivos en el mismo directorio son las llaves del servicio onion, y es fundamental que se mantengan de forma privada.

Si tus llaves privadas son expuestas, entonces otra gente puede hacerse pasar por tu servicio onion, considerandolo comprometido, inútil y peligroso para visitarlo. Ahora puedes usar el navegador Tor para conectarte a tu servicio onion!

Mas Recursos

Como siguiente paso, puedes habilitar Onion-Location y de esa forma publicitar tu sitio onion para todos los usuarios del navegador Tor que usen tu sitio web:

`https:/community.torproject.org/es-AR/onion-services/advanced/onion-location/`

Si es la primera vez que tu amigue usa servicios Onion, compartirles el Manual de Usuaria del navegador Tor:

`https://tb-manual.torproject.org/es/onion-services/`

Es también posible hacer un servicio Onion extra privado, protegido por una clave privada y un usuario para autorización. Leer mas aqui:

`https://community.torproject.org/es-AR/onion-services/advanced/client-auth/`

PORQUE USAR ONIONS?

Descentralización
No hay una autoridad central que apruebe o rechase servicios onion. La direccion de un servicio onion es generada automáticamente. Las operadoras no usan una infraestructura DNS regular y no necesitan comprar o registrar un nombre de dominio.

Eliminación u ocultamiento de metadatos
Cuando tu usas la red Tor para navegar la web, no estás enviando por defecto ninguna información de quién eres o desde donde te conectas. Los servicios onion usan la red Tor para eliminar información sobre donde están situados. Al usarlos se eliminan todos los metadatos que pudieran, de otra forma, estar asociados al servicio.

Sostenibilidad de la red
Los servicios onion no usan el mismo circuito que las conexiones regulares de Tor. El tráfico que generan nunca sale de la red de Tor, y por lo tanto estos circuitos liberan ancho de banda de los relays de salida para otros usuarios de la red. Más allá de esto, cuando un servicio está disponible mediante servicios onion, agrega diversidad a la red de Tor. Usa un conjunto diferentes de circuitos en la red, evitando los relays de

Elevar la privacidad de tu servicio
Mas alla de sitios web y onion, es posible hacer muchas otras cosas con servicios onion, por ejemplo, correo electrónico.

Libertad de prensa y evasión de censura
Las conecciones normales de Tor ya permiten evadir censura, pero solo los servicios onions pueden anonimizar las dos partes de la comunicación - usuarios y proveedor-, creando un canal de comunicación libre de metadatos entre el usuario del servicio y el servicio mismo.

Diferentes actores alrededor del mundo, como gobiernos y proveedores de Internet, implementan tecnologías de censura para bloquear acceso a prensa independiente así como a herramientas para privacidad. En los últimos años, para proteger libertad de expresion y opinion en lugares donde hay censura, varios medios de prensa han puesto disponibles sus sitios web sobre servicios onion.

Este es el caso de NY Times, ProPublica, Deutsche Welle, BBC, The Markup y otras redacciones.

Proteger fuentes, informantes y periodistas
Muchos periodistas y medios de prensa usan herramientas basadas en servicios onions para proteger a sus fuentes. Ellas usan herramientas como SecureDrop, GlobaLeaks, or OnionShare para compartir y aceptar documentos de fuentes anónimas.

Educar usuarios sobre privacidad por diseño
Los servicios onion son un perfecto ejemplo de tecnología diseñada con privacidad en mente, donde uno es seguro y anónima por defecto. Hacer tu servicio disponible sobre servicios onion es una oportunidad para educar al público en general sobre Tor y cuanto más seguro puede ser el acceso a internet: tan fácil como navegar una página web.

¡Recuerda, una cebolla por dia mantiene a la vigilancia lejos!