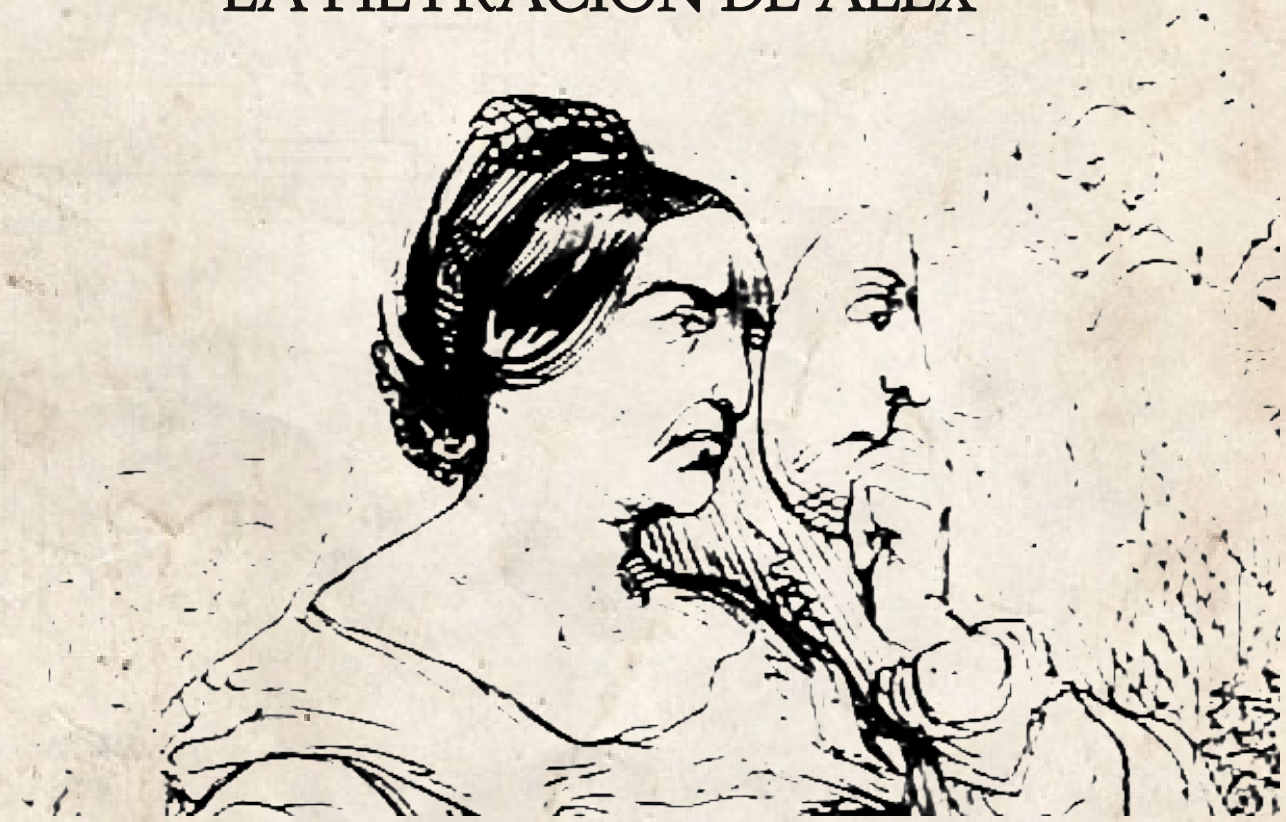
LA FILTRACIÓN DE ALEX



MANUAL DE SEGURIDAD CREADO EN HUELVA POR HATON, LULZCAT, FANTA Y MARI.

"LA VIDA ES MUY PELIGROSA. NO POR LAS PERSONAS QUE HACEN EL MAL, SINO POR LAS QUE SE SIENTAN A VER LO QUE PASA"

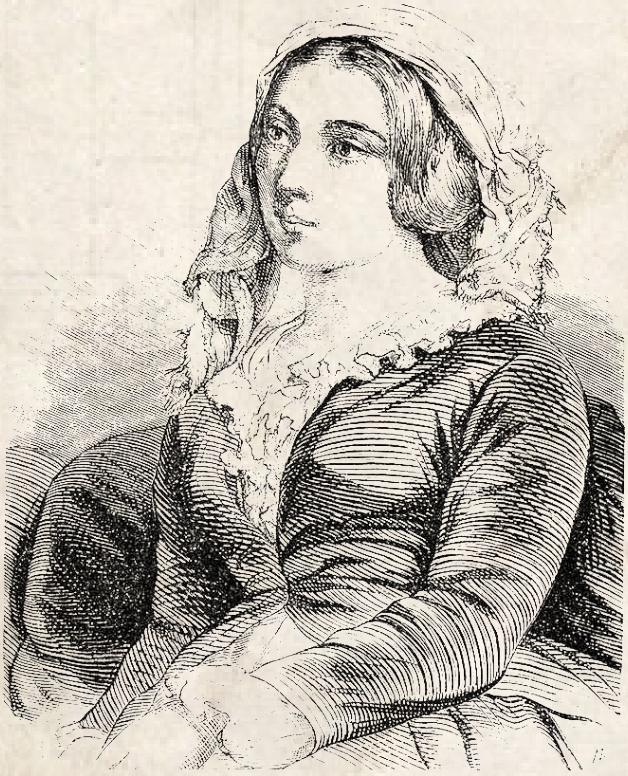
Albert Einstein

Introducción

La luz de la nevera ilumina la cocina cuando recoges la sexta o séptima cerveza. En realidad has perdido la cuenta hace un buen rato.

Miras a tu alrededor mientras cierras la puerta del frigorifico en busca del abridor y lo encuentras finalmente rebuscando bajo un montón de latas vacías y restos de embases de comida basura a domicilio.

Regresas al salón y enciendes el ordenador. El ordenador va bastante lento pese a que lo compraste hace apenas un par de meses. En el monitor se empieza a visualizar una foto en la que aparece tu hija, tu expareja y tu. Arrancas a llorar una vez más ya que te vienen a la mente viejos momentos cuando aún érais una familia unida.



El reloj de cuco situado a la izquierda de la chimenea marca la media noche. Tras un buen rato navegando entre titulares decides escribir un email a tu hija ya que nunca te coje el teléfono.

En la bandeja de entrada ves cientos de correos sin leer pero uno en especial te llama la atención. Procede de un remitente desconocido y no tiene asunto aunque lleva un adjunto basante pesado.

Estás confusa, no sabes que hacer...

 # ¿Prefieres ir a buscar otra cerveza mientras se descarga el adjunto? Pasa a la p. 5
 # ¿Prefieres eliminar el correo e ir a dormir de una vez? Pasa a las p.6

En busqueda de otra cerveza

Estás demasiado borracha y cansada. Por un momento piensas en eliminar el correo e ir a dormir pero finalmente decides tomar la penúltima y ver que es aquello.

En el trabajo, las compañeras siempre te han recomendado que no uses POP para bajar el correo y que es mejor usar 'nosequé' otra cosa. Lo cierto es que no sabes si es mejor una cosa u otra ni de que demonios hablan. Lo que sabes es que cuando bajas un correo desaparece del servidor y luego desde el trabajo ya no puedes verlo.

El motivo de comprar el portátil fue para llevar siempre el correo contigo y no tenerlo separado en diferentes ordenadores pero al final usas más el sobremesa.
Ya que tu trabajo te obligaba a estar permanentemente en la línea prematura de las noticias informativas, a la caza de cualquier pieza de la realidad que sirviera para hacer noticia y por tanto poder traficar con ella.

Mientras el archivo va descargándose a tu disco duro empiezas a recordar el día en el que tu hija dejó completamente de dirigirte la palabra y lloras de nuevo.
Tu hija de 17 años perdió el ojo en aquella manifestación y tu no hiciste nada por miedo a perder tu trabajo en el periódico. Aceptaste el dinero que se te ofrecía por tu silencio. Piensas que ella perdió el ojo por juntarse con esas malas amistades de perroflautas antisistema de los que bastantes veces le advertiste.

Finalmente el archivo se descarga. Empiezas a examinar el contenido y enseguida entiendes que se trata de información sobre personas. Fotos, dirección de residencia, vínculos familiares, edad, lugar de nacimiento, ... pero finalmente visualizando el contenido de un fichero llamado numeros.csv, entiendes que no se trata de personas. Son policías.

El número de placa de miles y miles de policías nacionales vinculada a sus datos personales empiezan a darte bastante miedo. No conoces la dirección de email que te manda esa información y buscando en la red no encuentras nada sobre ella.

De repente sientes una sensación de ahogo en la garganta, la respiración entrecortada, un pellizco en el estómago, y una sensación de paranoia aguda se cruza en tu cabeza. Cientos de pensamientos se agolpan, miles de problemas que tienes que solucionar para guardar tu seguridad te esperan.

Te ha pasado más de una vez y has perdido información por no tener copias de seguridad. Sabes la importancia que tiene esta filtración tanto para ti como para mucha gente. Empiezas a buscar en lal red y encuentras una web llamada elbinario.net. En ella hay un articulo sobre copias de seguridad y encuentras que recomiendan algo llamado cifrado.

Estás nerviosa, sabes que esa información puede ser peligrosa. Pero quieres conservarla y sigues investigando. Sigues mirando la entrada y ves que el cifrado oculta la información gracias a una clave. Parece de película pero también puedes hacerlo tu. Recomiendan un programa llamado TrueCrypt. Parece simple de usar y entiendes que TrueCrypt permite guardar información en algo llamado "tumba".

 # ¿Decides hacer una copia de seguridad usando TrueCrypt? Pasa a la p. 8
 # ¿Prefieres hacer una copia de seguridad sin cifrar? Pasa a la p. 7

Antes de ir a la cama

Estás demasiado borracha y cansada. Por un momento piensas en eliminar el correo e ir a dormir pero finalmente decides tomar la penúltima y ver que es aquello.

En el trabajo, las compañeras siempre te han recomendado que no uses POP para bajar el correo y que es mejor usar 'nosequé' otra cosa. Lo cierto es que no sabes si es mejor una cosa u otra ni de que demonios hablan. Lo que sabes es que cuando bajas un correo desaparece del servidor y luego desde el trabajo ya no puedes verlo.

El motivo de comprar el portátil fue para llevar siempre el correo contigo y no tenerlo separado en diferentes ordenadores.
Ya que tu trabajo te obligaba a estar permanentemente en la línea prematura de las noticias informativas, a la caza de cualquier pieza de la realidad que sirviera para hacer noticia y por tanto poder traficar con ella.

Mientras el archivo va descargándose a tu disco duro empiezas a recordar el día en el que tu hija dejó completamente de dirigirte la palabra y lloras de nuevo.
Tu hija de 17 años perdió el ojo en aquella manifestación y tu no hiciste nada por miedo a perder tu trabajo en el periódico. Aceptaste el dinero que se te ofrecía por tu silencio. Piensas que ella perdió el ojo por juntarse con esas malas amistades de perroflautas antisistema de los que bastantes veces le advertiste.

Finalmente el archivo se descarga. Empiezas a examinar el contenido y enseguida entiendes que se trata de información sobre personas. Fotos, dirección de residencia, vínculos familiares, edad, lugar de nacimiento, ... pero finalmente visualizando el contenido de un fichero llamado numeros.csv, entiendes que no se trata de personas. Son policías.

El número de placa de miles y miles de policías nacionales vinculada a sus datos personales empiezan a darte bastante miedo. No conoces la dirección de email que te manda esa información y buscando en la red no encuentras nada sobre ella.

De repente sientes una sensación de ahogo en la garganta, la respiración entrecortada, un pellizco en el estómago, y una sensación de paranoia aguda se cruza en tu cabeza. Cientos de pensamientos se agolpan, miles de problemas que tienes que solucionar para guardar tu seguridad te esperan.

Te ha pasado más de una vez y has perdido información por no tener copias de seguridad. Sabes la importancia que tiene esta filtración tanto para ti como para mucha gente. Empiezas a buscar en lal red y encuentras una web llamada elbinario.net. En ella hay un articulo sobre copias de seguridad y encuentras que recomiendan algo llamado cifrado.

Estás nerviosa, sabes que esa información puede ser peligrosa. Pero quieres conservarla y sigues investigando. Sigues mirando la entrada y ves que el cifrado oculta la información gracias a una clave. Parece de película pero también puedes hacerlo tu. Recomiendan un programa llamado TrueCrypt. Parece simple de usar y entiendes que TrueCrypt permite guardar información en algo llamado "tumba".

 # ¿Decides hacer una copia de seguridad usando TrueCrypt? Pasa a la p. 8
 # ¿Prefieres hacer una copia de seguridad sin cifrar? Pasa a la p. 7

Copia de seguridad sin cifrar

No tienes tiempo de tonterias de esas de cifrar información. Es algo ridiculo piensas y por tanto simplemente copias los archivos que te han mandado por email al pendrive donde durante años has estado almacenando las fotos de las vacaciones familiares.

Estas muy cansada y te llevas el pendrive en el bolsillo de tu pantalón hasta tu habitación.

Al día siguiente usas los mismos pantalones y sales a la biblioteca a buscar un libro con el que distraerte y evadirte.

Pierdes el pendrive en la biblioteca. Un estudiante lo encuentra y se lo guarda.

El estudiante va a su casa y ve la información. Es un estudiante de informática con padre policia.

El estudiante se hace copia y entiende enseguida que es importante identificar a quien ha perdido ese pendrive.

Para ello lo que hace es primero una copia de seguridad del pendrive en su disco duro y despues le pasa varios programas de recuperación de datos donde recupera las fotos de tu familia.

En cuestión de días la policia llega a tu casa y te detienen para interrogarte.

Fin

Cifrando la copia de seguridad

Optas por cifrar un pendrive que anda por casa ya que consideras que la información es sensible y si se perdiese podría poner en peligro a bastante gente. Tras una sencilla busqueda en el buscador web duckduckgo.com accedes la web Oficial http://www.truecrypt.org desde donde descargas ese programa. Simplemente ejecutandólo ya se abre. Unos simples pasos te llevan a conseguir un cifrado robusto (para mucha gente salvo lo mismo para la NSA) del dispositivo. Era algo así:

Crear volumen ->> Crear volumen en una partición >> dispositivo >> Crear un volumen Estandar >> Seleccionar el dispositivo >> Algoritmo cifrado: AES - Twofish - Serpent >> Hash: SHA-512 >> PASSWORD.

Finalmente formateas la unidad.

El formateo de la unidad, según has leído, borra bien los datos que había en ella. Por lo que te lleva varias horas. Dejas el ordenador encendido y te vas a dormir.

A la mañana siguiente ya tienes el dispositivo formateado e introduces los archivos en el pendrive.

Has leido por internet que TrueCrypt lo mismo no es tan seguro como comentaban y que es posible que este comprometido por lo que antes de meter los datos al pendrive decides empaquetarlos una vez más y dejarlos bien cifrados con gpg por si las moscas.

Además de esconder el pendrive bien debajo de esa baldosa suelta que tienes en el baño. Te das cuenta de que si te encuentran esa te quedas sin los datos y por tanto decides crear otro pendrive con los datos cifrados.

Lo mismo estas siendo demasiado paranoica piensas. Empiezas a darle vueltas en la cabeza a la importancia que podría tener esa información y te planteas la siguiente pregunta:

¿Era la contraseña suficiente robusta?

Sí, la contraseña era segura ve a la p. 29
No, la contraeña no es segura ve a la p. 9

Comprobando la clave

Consideras que la contraseña es lo suficientemente segura no obstante prefieres comprobarlo por si las moscas.

Algunas veces no importa si tienes una buena y larga si no sabes como ni donde la metes y por tanto optas por leer las viejas recomendaciones a la hora de seleccionar claves que te dejó el informatico anotadas hace años en la anterior empresa para la que trabajaste.

Las recomendaciones eran las siguientes:

- No has de usar claves que existan en algún diccionario. Ejemplos: perro, gato, universidad.

- No has de usar claves que lleven el nombre de algún conocido. Ni el de tu novio, ni el de tu mascota, ni el de tu hijo/hija.

- Nada que tenga que ver contigo. Si eres un fan de Reincidentes pues haz el favor que tu clave no sea el nombre del grupo o de algún disco o canción. Las claves no han de tener nada de sentido ni nada que nos vincule a ellas.

- Nada de contraseñas con números de teléfono. Eso es ridículo. Una password numérica saldrá rápido.

- Nunca has de usar la contraseña que te dan por defecto. Si algún cacharro (un router por ejemplo) viene con la clave 1234 o admin has de cambiarla.

- No repitas la misma clave en ningún sitio. Si tienes la misma clave en tu cuenta de faceboook y tu correo van a entrarte al facebook y al correo.

- Es importante que las contraseñas contengan tanto números como letras mayúsculas y minúsculas. Al mismo tiempo han de llevar caracteres "raros" como pueden ser el "." o "#".

Compruebas tu clave en base a las recomendaciones y cumple. Decides salir a patinar un rato para distraerte y despues de patinar te vas al trabajo tras una refrescante ducha.

Llegando a casa

Llegas a casa tras un día agotador, cansada , deseando tumbarte en la cama y caer en un sueño profundo, apenas puedes introducir la llave en la cerradura y cuando lo consigues, abres la puerta y observas perpleja como todo el salón está alborotado con todas tus cosas desordenadas y revueltas.

Buscas rápidamente aquellos objetos de valor que sueles utilizar en la vida diaría. Y echas en falta tu portátil, discos, memorias externas. Recuerdas aquel otro pendrive que cifraste y escondiste tras las baldosas del baño. Corres rápidamente hacia el y ves que aquella baldosita rota que no encajaba muy bien en la pared está vacía.

Rápidamente recuerdas que el segundo pendrive que cifraste con toda la información se encontraba en tu bolsillo. Compruebas todos los bolsillos del pantalón y por fin lo encuentras, suspirando con tranquilidad.

Caes en el sofá derrotada por el susto que acabas de recibir y piensas en que menos mal que el primer pendrive se encontraba cifrado.

Por la mañana llamas a aquel amigo informático, Rodolfo, que siempre te acaba sacando de todos los líos que no sabes resolver con el ordenador. Le cuentas lo ocurrido y él decide prestarte y ponerte a punto un portátil viejo con Debian GNU/Linux como sistema operativo por lo que mientras esperas a que venga utilizas para leer el correo tu smartphone moderno.

Sin poder conciliar el sueño decides seguir bebiendo de la litrona. La terminas y abres un par de ellas más.

Entrada la medianoche recibes un nuevo correo anónimo. Muy breve, conciso y con instrucciones muy directas:

Visita la siguiente web, hay información útil para ti que te ayudará a entenderlo todo: www.xqz3u5drnyuzhaeo.onion.

Extrañada, pinchas en el link, pero no eres capaz de ver la web. Lees un mensaje como el siguiente:

Servidor no encontrado
Firefox no puede encontrar el servidor en www.xqz3u5drnyuzhaeo.onion.

Los primeros rayos de sol juguetean a través de la ventana, despertándote ese juego de luz y sombra. Mientras preparas el café matutino llamas a Rodolfo, tu amigo informático, para que te enseñe a ver cuál es el problema:

- Hola, ¿qué tal Rodolfo?
- Hola, Alex, ¿qué hay?
- Mira, siento darte la lata de nuevo pero el navegador no me funciona
- ¿Qué dirección te entra? ¿DuckDuckGo?
- A ver, déjame mirar (teclea duckduckgo en el navegador), Sí! sí que va el pato
- ¿Cuál es la dirección qué quieres ver?
- Pues son muchas letras y números acabados en .onion
- Ah! pues eso es un dominio .onion, tendrás que instalarte Tor.

Llegando a casa

- ¿Y cómo lo hago?
- A la tarde me paso por tu casa.

Llaman al timbre. Es Rodolfo y parece bastante sorprendido contigo.

Rodolfo lleva toda la vida enamorado de ti y es llamarle y venir como un rayo. A ti Rodolfo no te gusta, es poca cosa. Un friki que a diferencia de tu ex pareja (el padre de tu hija) Rodolfo no tiene un tatuaje de letras chinas en el cuello, no toma batidos en el gimnasio ni se viste con ropa moderna pero no cabe duda de que siempre ha estado contigo en los momentos complicados.

Nunca te ha gustado Rodolfo. No es guapo, tiene cara de perro pero eso si, tiene un gran corazón.

Es una persona inteligente y muy observador. Rodolfo se percata instantaneamente al entrar a tu casa de que estas pasando un mal momento.

Tu casa huele mal ya que llevas mucho tiempo sin salir demasiado. Sales solamente a comprar bebida alcoholica y practicamente todas las habitaciones tienen alguna lata o litrona a medias.

- ¿Qué demonios te esta pasando? - Pregunta Rodolfo

Le comentas que no estas en tu mejor momento y te disculpas con Rodolfo por aceptar aquel soborno de la policia para guardar silencio cuando tu hija quedó sin ojo en aquella manifestación.

Rodolfo te dijo que no aceptases.

- Rodolfo, he cambiado, he visto la luz y ahora entiendo que fue todo un error. - Le dices
- Alex, no tienes que darme explicaciones. Me alegra que estes arrepentida. Aquí me tienes para lo que haga falta, para lo bueno como para lo malo.
- Gracias Rodolfo, eres una buena persona. Es una pena que no lleves tatujae de letras chinas en el cuello con tu nombre y no fumases porros de joven. A mi siempre me han gustado los malotes como bien sabes.
- Si, lo se pero yo no soy un malote de esos modernos. Lo siento Alex.
- Ohh Rodolfo, eres siempre tan comprensivo conmigo. Mil gracias por el equipo con el sistema operativo ese raro.
- ¿Sistema raro?
- Si, GNU/Linux Debian.
- Ahh, no lo he instalado. He pensado que era mejor que me ayudases con eso y así puedes aprender el procedimiento.
- Ok. Preferiria en realidad que tu hicieses todo el trabajo y me lo dieses realizado pero no puedo pedirte eso.
- Puedes hacerlo querida Alex pero preferiria que lo aprendieses.
- Si no queda otro remedio empecemos ya mismo.

Lo cierto es que Rodolfo de vez en cuando se solía pasar por tu casa cuando tu ex-marido estaba en el trabajo y te hacía un repaso y limpieza de virus pero era algo que en realidad querías aprender a hacer. Depender de Rodolfo siempre era un error. Era mejor que lo aprendieses por ti misma.

Llegando a casa

Rodolfo se puso a instalar Debian.

Me comentó que lo primero de todo era bajarse una ISO. Una ISO al parecer era un archivo que bajabas de la web debian.org y grababas en un CD por ejemplo. El ya tenía la iso esa moderna en un CD por lo que simplemente lo puso en la unidad y apagó y encendió el equipo.

Rodolfo se estaba portando muy bien. No solamente me estaba dejando uno de sus ordenadores sino también me estaba aconsejando sobre cifrar el disco duro por si me robaban otra vez que al menos no viesen mi información.

Los pasos para instalar ese sistema operativo tras meter el CD eran los siguientes:

- Install
- Selecionar idioma: spanish
- Seleccionar España.
- Seleccionar Español.
- Configurar la red. Seleccionar tarjeta de red.
- Poner nombre de la maquina: No pones algo que te identifique.
- Nombre dominio en blanco.
- Clave del superusuario (recuerdas los criterios para una buena clave).
- Configuar una cuenta de usuario (no poner tu nombre)
- Zona horaria, en este caso peninsula.
- Particionado de disco. Seleccionar guiado, utilizar todo el disco y configurar LVM cifrado.
- Seleccionar el disco a particionar.
- Esquema de particionado. Todos los ficheros en una partición (recomendado para novatos).
- Deseas guardar los cambios y configurar LVM. Se le responde que si.
- Comienza el tema del particionado del disco duro. El cifrado.
- Instalando el sistema base.
- Configurar el gestor de paquetes. ¿Utilizar una replica de red? Sí.
- ¿Usar software no libre? No.
- Instalar el cargador de arranque grub en un disco duro. Decimos sí.

Una vez instalado el sistema abres una cerveza e invitas a Rodolfo a otra. Te preparas para instalar TOR siguiendo las indicaciones de Rodolfo.

Parece ser que una de las aportaciones del proyecto TOR es Tor Browser Bundle (TBB de ahora en adelante). Se puede descargar desde aquí: https://www.torproject.org/index.html.en

TBB es una versión del navegador web "Firefox" modificada para que sus conexiones pasen por la red TOR. TBB además viene con configuraciones y plugins que hacen la navegación más segura.

Llegando a casa

Para ejecutar TBB en Debian Linux debemos seguir tres pasos:

Descargar desde https://www.torproject.org/index.html.en

Descomprimir: tar -Jxf archivo.tar.xz*

Ejecutar. Doble click sobre start-tor-browser o lo ejecutamos desde la terminal. ./start-tor-browser

En caso de que no funcionase la descompresión es posible que sea que necesites instalar el paquete xz-utils.

El comando: apt-get install xz-utils servirá para instalarlo.

Si lo que uno desea es instalar TOR en Debian sin necesidad de instalar Tor Browser Bundle esto se puede realizar simplemente con el comando: apt-get install tor y después configurar sus navegadores y aplicaciones manualmente para obtener mayor control de lo que se esta haciendo.

Algunos Consejos

- Descargarse la versión en inglés. La mayoría de la gente usa la versión en inglés, eso permite dar menos información sobre nosotros.

- Ten en cuenta que solo se pasa por TOR con TBB. Una conexión realizada, por ejemplo, desde Pidgin o Thunderbird, no pasa por TOR, por lo que la conexión se hace desde tu IP. Es posible "torificar" estos programas de todos modos.

- No instales plugins en TBB.

- Usa HTTPS siempre que sea posible.

- No abras archivos descargados desde TBB. Un doc o un pdf pueden requerir archivos de la red. Al no pasar ese proceso por TOR, podrían ver tu IP.

Tras instalar tor visitas aquella dirección tan rara. Perpleja empiezas a reconocer la escena; una carga policial en una manifestación , tu hija corriendo delante de la carga, se vuelve y grita:

- !Hijos de Puta! - y tras ello una bala de goma impacta en su cara, haciéndola sangrar.

En aquel fatídico día perdió su ojo. Sentiste rabia porque la indemnización que habÍas recibido compró tu silencio terminando por consentir lo de aquella terrible tarde.

Empiezas a ver el vídeo una y otra vez , buscando detalles, analizando fotograma a fotograma, hasta que finalmente das con la imagen: Su rostro, el número de placa, y su pistola escupiendo bolas de goma que azotaban a todos los manifestantes.

Llegando a casa

! Le tienes! Él es el culpable de truncar la vida a tu hija, y ahora sólo puedes pensar en que esos datos que te llegaron vean la luz para que alguien se tome la justicia por su mano.

Llamas a tu hija por teléfono inmediatamente, tras algunos meses sin hablar, todas esas llamadas perdidas te hacen buscar otra alternativa por la cual comunicarte, recuerdas aquel número de su mejor amiga, le mandas un mensaje pidiéndole alguna forma de contactar con tu hija, y te pasa su dirección de jabber:

cafeina@jabber.org

- Ella siempre está ahí localizable- asegura.
- Pero ... ¿qué es eso de jabber? ¿le mando un correo?
- No, bájate algún sistema de mensajería XMPP, tipo pidgin, y añade la cuenta de tu hija.

Así que quieres crearte una cuenta en un server jabber y encuentras un largo listado donde poder hacerlo:

suchat.org
elbinario.net
is-a-furry.org
jabber.ab-storm.de
webchat.chatme.im
duck.co
linuxlovers.at
tfsfe.org
jabber.ccc.de
creep.im
palita.net
jabb3r.net
neko.im
mijabber.es

Decides abrir una cuenta en mijabber.es.

https://mijabber.es/jappix/

Rellenas los datos en la web. Siempre te gustaron mucho las madalenas, así que creas la cuenta de

madalena@mijabber.es

Ayer, andando por la calle, vistes un cartel que anunciaba un taller de Jabber usando cifrado, en un CSOA.

¡Perfecto! Es justo lo que necesitas para contactar con tu hija y es precisamente mañana. Te vas a descansar con ansias de hablar con ella.

Llegando a casa

Te despiertas, bajas al bar de abajo a tomar un café. Aunque no te sientes muy cómoda te das cuenta de que quizás esos antisistema tenían algo de razón.

Coges el portátil con Debian que te dió tu amigo y vas hacía el centro social. Allí te encuentras un grupo de personas que le llaman a esa habitación hacklab. Tienen cacharros electrónicos que parecen muy interesantes.

Empieza el taller y hacéis una ronda de presentación. Te presentas como los demás, sin dar información sobre la filtración. Seguidamente empiezan a proyectar la instalación. La chica que da la charla abre una de esas pantallas negras e introduce tres comandos que realizan la instalación:

su
apt-get update
apt-get install pidgin pidgin-otr

Mientras se termina de descargar le echas un chorrito de coñac al café y... abres el software que tienen como icono una especie de pollito.

Los pasos para la configuración de la cuenta son los siguientes:

Cuando termina de descargarse e instalarse ejecutamos pidgin para configurar nuestra cuenta.

En la pestaña “Cuentas” hacemos clic sobre “Gestionar cuentas” para después presiona el botón “Añadir”:

Protocolo: XMPP
Nombre de usuaria: madalena
Dominio: mijabber.es
Contraseña: **********

Activación de pidgin-otr:

Herramientas >> Complementos
Se activa "Mensaje Fuera de Registro OTR"

Ya tienes todo listo para charlar con tu hija.

¿Decides cifrar la conversación con tu hija? Pasa a la página. ve a la p. 17
¿Prefieres no cifrar y seguir de forma insegura en plano? ve a la p. 16

Cifrar no parece ser una opción

Es muy importante contactar con tu hija pero es como si no quisiera hablar más contigo. Las llamadas teléfonicas que has realizado siempre son ignoradas.

Abres el programa ese del icono con un "pollo" o una paloma.

Se llama en realidad "Pidgin". Hablas con tu hija pero ella no quiere responder.

Decides abrir otra lata de cerveza que terminas rápidamente de beber. Sigue sin contestarte al teléfono.

Ahora vas a por una botella de vino y al regresar ves que ha contestado. El mensaje es

- Quien quiera que seas has de cifrar.

Al fin de cuentas tras una borrachera enferma y una mañana de resaca, optas por aprender a cifrar.

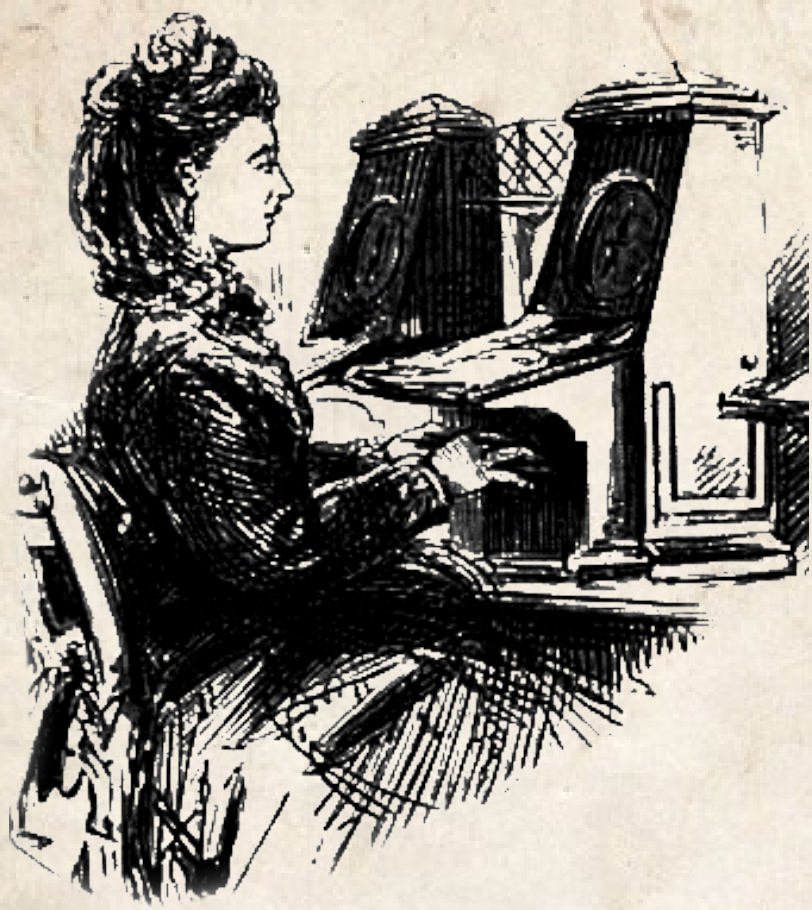
Deseas aprender a cifrar la mensajeria instantania. Ve a la página 17.

Conversación cifrada con tu hija

Llegas a casa y lo primero que haces es encender el portátil que te ha dejado Rodolfo. Te conectas a tu cuenta de Jabber y allí tienes a tu hija conectada. La saludas cifrando la conversación:

21:05:10 - madalena: Hija, ¿cómo estás?
21:05:34 - madalena: soy tu madre
21:06:05 - cafeina: mamá?
21:06:15 - madalena: sí, tengo una cosa importante que contarte
21:06:22 - cafeina: qué ha pasado?
21:06:22 - madalena: sé que me he equivocado
21:06:36 - madalena: siento haber tardado tanto en darme cuenta..
21:06:44 - cafeina: qué pasa??
21:07:25 - madalena: no se si es el mejor método de decirtelo
21:08:01 - madalena: no se si este medio es seguro
21:08:19 - cafeina: sí mamá, esto está cifrado
21:09:06 - cafeina: qué ocurre, me estás preocupando
21:09:16 - madalena: me ha llegado una filtración muy importante
21:09:28 - cafeina: sobre qué?
21:09:47 - madalena: me ha llegado una lista
21:09:52 - madalena: un listado muy grande
21:10:00 - madalena: todos los nombres, fotografias, direcciones, telefonos
21:10:02 - madalena: correos
21:10:07 - madalena: de la policia
21:10:25 - cafeina: de verdad?
21:10:29 - madalena: sí
21:10:32 - madalena: y para mas inri
21:10:37 - madalena: me han enviado un vídeo
21:10:42 - madalena: dónde se ve lo que te pasó
21:10:45 - cafeina: Eso es bastante importante...
21:10:53 - cafeina: a mi??
21:10:57 - madalena: sí
21:11:00 - madalena: sabemos quien fue
21:11:25 - cafeina: qué sale en el vídeo concretamente?
21:11:41 - madalena: el policia disparando la pistola
21:11:47 - madalena: y se ve su número de placa
21:11:51 - madalena: con los datos de la filtración sabemos quien es
21:12:30 - cafeina: hace cuánto de esto?
21:12:42 - madalena: unos días
21:12:49 - madalena: estoy investigando como mantener eso seguro
21:13:04 - madalena: y no comprometernos ni nosotras ni la fuente
21:13:10 - cafeina: ok
21:13:22 - cafeina: lo vas a filtrar a las redes sociales no?
21:13:27 - madalena: no lo se
21:13:40 - cafeina: cómo que no lo sabes?!
21:13:56 - cafeina: eso tiene que ver la luz

Conversación cifrada con tu hija



21:14:13 - cafeina: podria ser una forma de defendernos
21:14:20 - cafeina: ante esos perros de mierda
21:14:29 - cafeina: que nos apalean sin motivo
21:14:29 - madalena: sí
21:14:35 - madalena: pero he estado pensando sobre ello
21:14:42 - madalena: quizás podría conseguir filtrarlo a algún periódico de tirada nacional
21:15:02 - madalena: con eso llegaríamos a mucho más público y una vez filtrado sería difícil de censurar
21:15:06 - madalena: por otra parte cabe la posibilidad
21:15:09 - madalena: de que si hiciésemos eso
21:16:15 - madalena: nos pongamos en peligro
21:16:22 - madalena: he pensado también
21:16:31 - madalena: que quizás eso podría servir a los movimientos sociales
21:16:38 - madalena: por ejemplo,
21:16:42 - madalena: recuerdas los escraches?
21:17:18 - cafeina: tienes que pasar esa info a las redes sociales, a los distintos grupos activistas
21:17:32 - cafeina: para que se le de un buen uso a esa info
21:17:41 - cafeina: y poder hacer algo útil
21:17:49 - cafeina: por la seguridad no te preocupes, mamá
21:18:27 - cafeina: te pondré en contacto con mi grupo activista para que te proporcione herramientas

Conversación cifrada con tu hija

21:18:36 - cafeina: y así estés más segura
21:18:41 - madalena: entonces ves mejor la opción de filtrarlo
21:18:45 - madalena: a los movimientos sociales?
21:18:53 - madalena: que a algún periódico digo
21:19:06 - cafeina: no te quepa duda!!
21:19:35 - madalena: perfecto
21:20:11 - madalena: entonces haremos eso
21:21:13 - cafeina: activistahumanitasta@jabber.org
21:21:39 - cafeina: es mi amigo, podrá ayudarte con todo lo que necesites
21:21:53 - cafeina: activistahumanista@jabber.org
21:22:06 - madalena: ok
21:22:09 - madalena: voy a agregarlo entonces
21:22:11 - madalena: gracias
21:22:12 - cafeina: pilota de todo el tema de filtraciones
21:22:29 - cafeina: y podrá ayudarnos
21:22:34 - cafeina: para que esa info vea la luz
21:22:42 - madalena: me gustaría verte
21:22:46 - cafeina: ya quedaremos
21:22:51 - cafeina: saludos mami
21:22:54 - cafeina: me alegro de verte
21:22:59 - cafeina: descansa y vigila
21:23:05 - madalena: que vaya bien hija
21:23:08 - madalena: un beso
21:23:17 - cafeina: ^^

Pasada la medianoche te aparece una notificación en pantalla. «activistahumanista@jabber.org en línea». ¡Perfecto! - piensas. Abres una conversación con él y empiezas a cifrar:

00:15:01 - madalena: Hola, soy la madre de cafeina.
00:16:29 - activistahumanista: Hola Alex. Lo sé, me ha puesto al día cafeina.
00:16:52 - madalena: ¿Qué vamos a hacer y como?
00:17:25 - activistahumanista: Ahora ando ocupado, mejor mandame todo a mi cuenta de correo: activistahumanista@openmailbox.org .Cifra con GPG please.
00:20:15 - madalena: No se muy bien como hacer eso pero bueno.

¿Quieres enviarle el correo usando GPG? ve a la p. 20
¿Quieres enviarle el correo en plano? ve a la p. 23

Correo cifrado con GPG

Lo primero que haces es acceder a la web que te ha recomendado activistahumanista:

https://openmailbox.org

Llegas allí y te abres una cuenta.
¡Qué fácil! solo hay que introducir tu nombre, el correo y la contraseña deseadas y un captcha.

Madalena introduces de nombre y madalena@openmailbox.org cómo correo.

Aún queda aprender a usar GPG. Pero bueno, sabes que el cifrado es muy útil y más en la situación en la que te encuentras. Buscas en la red algún tutorial de cómo hacerlo. Encuentras uno que explica como instalar Thunderbird con el complemento Enigmail.

Lo sigues y parece fácil, te generas tus claves GPG y le envías los archivos cifrados con doble capa de cifrado.

Por un lado cifras con clave simétrica, esa en la que solo utilizas una password. La cifras con la que te compartió él en la conversación de Jabber. Es simple cifrar según has leído, simplemente es usar el comando gpg e introducirle la contraseña.

```
gpg -c información.pdf
```

Aprendes que para descifrarlo es simplemente usar el comando gpg seguido del archivo e introduces la contraseña.

```
gpg información.pdf.gpg
```

Por otro lado con el complemento Enigmail cifras el correo entero y el archivo con la clave pública de activistahumanista. Tienes la certeza que solo podrá ver el contenido él. Le envías el correo.

Al día siguiente recibes un correo:

> Hola madalena,
> me ha parecido muy interesante la información que me enviaste. La he estado analizando y parece que si se filtrase pudiera salir perjudicada alguna gente. Aparece información en los metadatos que podría delatarlos. Por eso te he limpiado los ficheros y te los he vuelto a enviar. Aquí tienes los ficheros cifrados con la clave de la otra vez.
>
> Espero que todo esto salga bien,
>
> Un abrazo, activistahumanista.

Parece ser que hay una cosa que se llaman metadatos. Habrá que buscar en el pato a ver qué es. Aparece un personaje curioso con un gorro, pero parece ser mejor sacar la información de la wikipedia.

Metadatos (del latín datum, 'lo que se da'), literalmente «sobre datos», son datos que describen otros datos.

Es decir, había información en la filtración sobre cosas aprecidas en ella. Supongo que debía ser la fecha, la hora e incluso el nombre de quien lo hizo. Curioso. Suerte que los ha borrado a ver si nos va a salir mal...

Decides enviarle un email a activistahumanista para ver si consigues ponerte en contacto con gente de los movimientos sociales.

- Al final han sido buena gente los perroflautas - piensas - debería dejar de llamarlos así...

> Buenas activistahumanista,
>
> Querría reunirme con gente de los movimientos sociales, para ver qué podemos hacer con la filtración. Tengo un par de cosas pensadas. ¿Podríamos reunirnos en algún sitio?
>
> Saludos,
>
> madalena

Te tomas la última cerveza de la noche. Van a ser unos días largos los que vienen.

- ¿Cómo he podido ser tan idiota? - dices en voz baja -. El cuerpo no te da para más y te quedas dormida en el sofá.

Te levantas al día siguiente. Miras el correo y ves que te ha llegado un mail de activistahumanista.

> Hola madalena,
>
> Voy a contacatar con algunos activistas. Si te parece nos vemos mañana en el canal #hactivistas en el servidor freenode a las 20:00h. Es importante que conectes cifrando. Hay un programa llamado xchat que permite hacerlo. En la red puedes encontrar algunos tutoriales.
>
> Nos vemos mañana,
>
> activistahumanista

¡A por ello! Abres en el navegador y te diriges al pato. https://duckduckgo.com aparece en la url. Te acuerdas de que alguien dijo que los enlaces en https van cifrados. Qué bien. «Instalar xchat debian». Te aparecen varios resultados, seleccionas el primero de ellos y aparece una instalación simple con ventanas. Parece fácil. Sigues los pasos y ya lo tienes instalado

Correo cifrado con GPG

Bajas a la calle a caminar un rato, necesitas que te de el aire, muchas emociones en tan pocos días. Te enciendes un cigarrillo mientras das un paseo por el barrio.

Qué responsabilidad sacar a la luz eso. Pero no puedes fallarle otra vez a tu hija. Son las 23:20 ya.

Empiezas a ir de camino a casa.

Enciendes el ordenador y abres xchat. Le das a conectar al servidor que te han indicado.

¿Decides usar cifrado (SSL) para conectar al servidor? Pasa a la página 24
¿Decides conectar al servidor sin cifrado? Pasa a la página 25

Cifrar es para ricos piensas

Esto empieza a ser un rollo. Tanto cifrado no es necesario piensas.

Esta gente vive en paranoia y no es para tanto por lo que decides enviar toda la información al email sin cifrarla.

Son unos paranoicos sin mejores cosas que hacer. No es para tanto. Piensan que les espian y no son tan importantes.

Despues de todo te vas a dormir.

A la mañana siguiente llaman a la puerta. Abres y es la policia.

FIN

En el IRC

Introduces la información en xchat y entras por el puerto 6697, cifrando.
Entras en el canal, parece que ya están hablando...

23:34 -!- madalena [~madalena@xx.xx.xxx.xxx] has joined #semananegra
23:34 < acthumanista> me parece guay
23:34 < acthumanista> bien
23:34 < madalena> hola
23:34 < acthumanista> cuentanos madalena, que pasa?
23:35 <@cafeina> sabes algo sobre quien te ha mandado la filtración?
23:35 <@cafeina> cuando te ha llegado el email?
23:36 < madalena> Me ha llegado mediante correo anónimo una filtración con datos: nombre, apellido, dni, número de placas, fotos de policías
23:36 < madalena> el email me llegó hace un par de días
23:36 < madalena> ni idea quién lo mando
23:36 < madalena> he estado borracha estos días, no sabría decirte
23:36 <@cafeina> mira please la dirección de mail
23:36 -!- alguno [~ning@xx.xx.xxx.xxx] has joined #semananegra
23:37 < acthumanista> te has acordado de entrar con ssl?
23:37 < madalena> asdf23@openmailbox.org
23:37 < madalena> sí, estoy con ssl
23:38 < acthumanista> cuenta lo del vídeo
23:38 < madalena> me ha llegado otro email con una dirección .onion
23:39 < madalena> ahí estaba el vídeo donde un policía disparaba con una bola de goma a mi hija
23:39 < madalena> ella perdió el ojo
23:39 <@cafeina> pero bien que no te importó aceptar el soborno.
23:39 -!- pepito [~fulanito@xx.xx.xxx.xxx] has quit [Ping timeout: 258 seconds]
23:39 < madalena> ya, todo el mundo comete errores...
23:40 < madalena> eso pretendo
23:40 < madalena> he pensado en que podríamos montar una web con la información de él
23:40 < acthumanista> dejaros de peleas ahora vale. sumar y no restar
23:40 < madalena> tenemos el vídeo, su foto, dirección y demás
23:40 < madalena> podríamos generar escraches
23:42 < acthumanista> no hables más
23:42 < acthumanista> parar.
23:43 < acthumanista> lo primero es pillar un dominio anonimo
23:43 < acthumanista> madalea
23:43 < madalena> debemos hacer algo. cómo se puede hacer eso?
23:43 <@cafeina> http://elbinario.net/2014/03/12/registro-de-dominios-anonimos/
23:44 <@cafeina> simplemente compra una de esas tarjetas con 20 euros por ejemplo de credito y regresas
23:46 <@cafeina> no te preocupes tu por la web.
23:47 < acthumanista> yo me ocupo de la web. Esta ya lista.

Bajas al 24 horas de la esquina a comprar la tarjeta. Pasa a la página 26

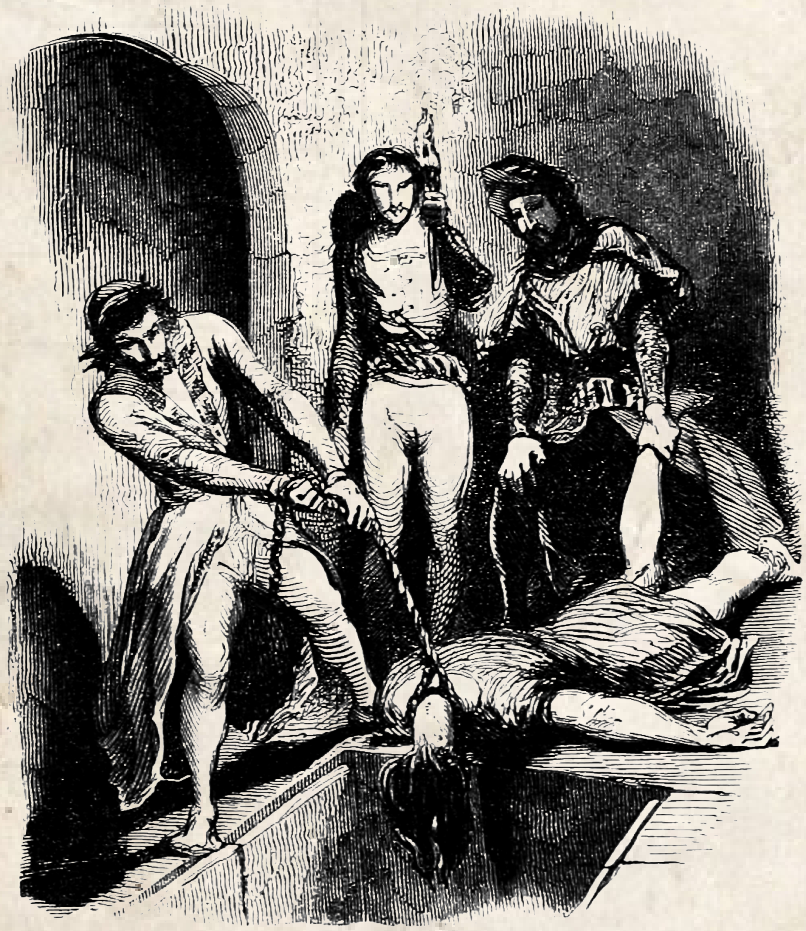
Conectas sin ssl al IRC.

Tus conversaciones están siendo enviadas en plano y tu IP canta dónde te encuentras y quien eres. No lo sabes, pero comprometes a todo el grupo activista donde te encuentras.

Ya te tienen localizada. A tí y a todos los que te rodean.

Qué cagada.

FIN



Registro de dominio

Sales a la calle a comprar una de estas tarjetas que permiten registrar dominios anónimamente.

Con paysafecard es posible adquirir dominios sin necesidad de dar tus datos.
Te han comentado que es sencillo el pago y que puedes encontrarlas en casi cualquier sitio de España.

Antes de salir has visitado la web: https://www.paysafecard.com/es-es/comprar/tiendas para comprobar donde tenias un punto de venta cercano.

Entras a la tienda, le pagas 30 euros y te dan una tarjeta con un número que tiene esa cantidad lista para gastar.

No has tenido que dar tu nombre y apellidos para ello ni dejar registro de ningún tipo.
Por lo visto un proveedor griego acepta paysafecard para registrar dominios desde http://www.papaki.gr/en

Regresas a casa y les das mediante jabber cifrando con OTR el número a activistahumanista.
Ellos se encargan de adquirir el dominio para la filtración.

Tiras una moneda al aire para ver si sale cara o cruz.

Si sale cara ve a la pág 28
Si sale cruz ve a la pág 27

Final I

Cada día bebes menos, ya no necesitas evadirte de la realidad, las cosas funcionan, empiezas a aceptar tu vida.

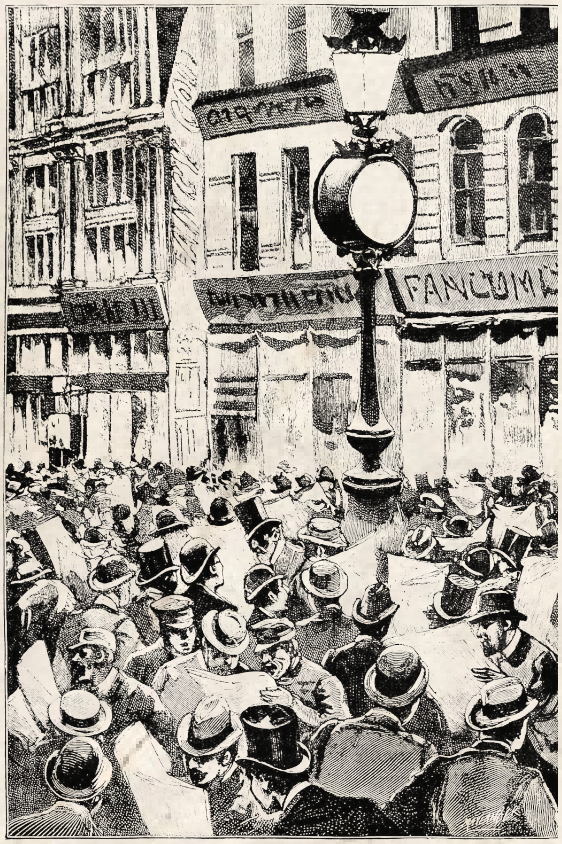
Tu hija te recibe con los brazos abiertos, algo que hacía años que no hacía. Lo que te llena de satisfacción y felicidad. Siempre buscaste su perdón pero sobre todo el perdonarte a ti misma y al fin lo consigues.

Finalmente la filtración del vídeo vió la luz, creando comandos antirepresivos que graban los abusos de la policía masivamente. Recurso que se presenta al parlamento europeo y censuran.

Ni un golpe más. Un colectivo Hacktivista filtra un docomento lleno de datos personales y datos familiares.

Se empiezan a hacer escraches en los casas de los policías. Las cosas parecen que funcionan, la gente parece que reacciona. Se acerca el cambio que todos teníamos en mente pero nadie sabía cómo efectuarlo. Sin saberlo, fuiste la gota que colmó el vaso e hizo a la gente levantarse contra los abusos del estado.

Rodolfo finalmente tiene las agallas de declararte su amor, y tu lo aceptas, porque sobre todo y ante todo es tu amigo, ese cariño especial que siempre le has tenido y nunca habías reparado en ello.



Final II

El documento se filtra pero no parece existir mucha reacción por parte de nadie.
La prensa no quiere líos y decide no publicar nada incluso los periódicos que se supone van de alternativos y pro movimientos sociales.

En determinados periódicos comienzan a salir noticias falsas sobre tu hija y al final la meten en la cárcel y a ti también. Todo el mundo piensa que eres una terrorista.

A ti te ingresan en un manicomio meses mas tarde.

Cuando finalmente te dejan en libertad ya no eres la misma persona no obstante abres un blog en Internet donde comienzas a hablar sobre los abusos del estado.

La gente no lee tu blog salvo para reírse. Te toman por loca y paranoica.

Comprobando la clave

Consideras que la contraseña es lo suficientemente segura no obstante prefieres comprobarlo por si las moscas.

Algunas veces no importa si tienes una buena y larga si no sabes como ni donde la metes y por tanto optas por leer las viejas recomendaciones a la hora de seleccionar claves que te dejó el informatico anotadas hace años en la anterior empresa para la que trabajaste.

Las recomendaciones eran las siguientes:

- No has de usar claves que existan en algún diccionario. Ejemplos: perro, gato, universidad.

- No has de usar claves que lleven el nombre de algún conocido. Ni el de tu novio, ni el de tu mascota, ni el de tu hijo/hija.

- Nada que tenga que ver contigo. Si eres un fan de Reincidentes pues haz el favor que tu clave no sea el nombre del grupo o de algún disco o canción. Las claves no han de tener nada de sentido ni nada que nos vincule a ellas.

- Nada de contraseñas con números de teléfono. Eso es ridículo. Una password numérica saldrá rápido.

- Nunca has de usar la contraseña que te dan por defecto. Si algún cacharro (un router por ejemplo) viene con la clave 1234 o admin has de cambiarla.

- No repitas la misma clave en ningún sitio. Si tienes la misma clave en tu cuenta de faceboook y tu correo van a entrarte al facebook y al correo.

- Es importante que las contraseñas contengan tanto números como letras mayúsculas y minúsculas. Al mismo tiempo han de llevar caracteres "raros" como pueden ser el "." o "#".

Compruebas tu clave en base a las recomendaciones y cumple. Decides salir a patinar un rato para distraerte y despues de patinar te vas al trabajo tras una refrescante ducha.

regresa a la página 10