Comunicaciones Secretas en Internet

Rafael Bonifaz <rafael@bonifaz.ec>

creative commons

https://privacidad.global/

¿Qué es la Privacidad?

creative commons

https://privacidad.global/

¿Quién puede vulnerar nuestra privacidad?

- Las grandes potencias
- Gobiernos locales
- Empresas de Internet
- Espionaje comercial
- Criminales
- Usuarios de redes sociales

Google

HackingTeam

facebook

creative commons

https://privacidad.global/

¿Quién Dice?

- 2011-2012 Spyfiles Wikileaks
- 2013 Documentos de Snowden
- 2015 FinFisher, HackingTeam
- 2016 Informe de Transparency Tool Kit: 18 países de Latinoamérica compraron software de vigilancia
- 2017 Gobierno Espía
- 2018 Cambridge Analytica, de Facebook
  Gelocalización de Google, Guatemala y ¡MÁS!
- 2019 ¿……..?

creative commons

La NSA y los Documentos de Snowden

"Yo, sentado en mi escritorio, tenía la facultad de intervenir al que fuera, desde un contador hasta un juez federal e incluso el presidente, siempre y cuando tuviera su correo electrónico personal"

creative commons

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

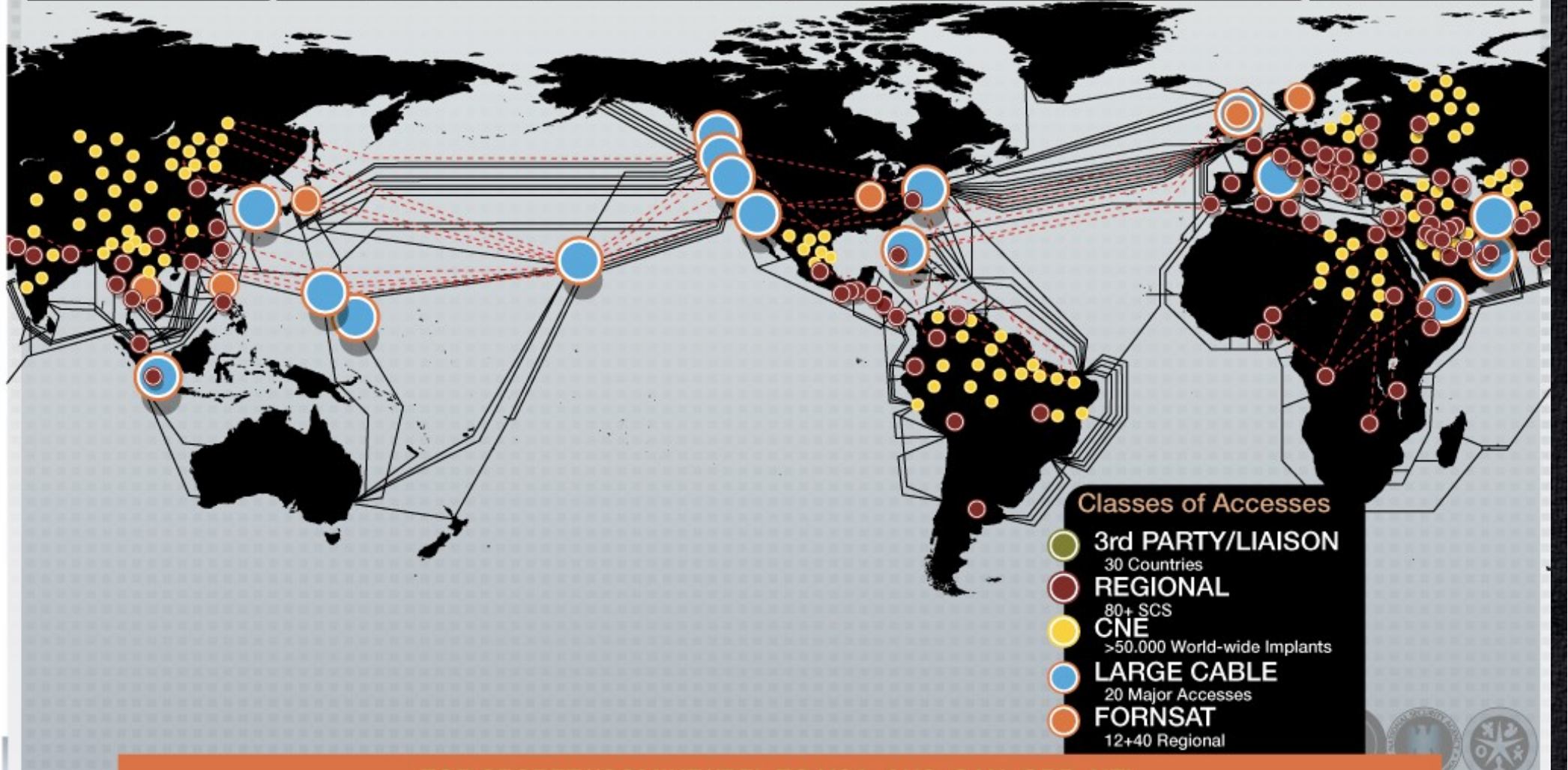
High Speed Optical Cable
Covert, Clandestine or Coorperative Large Accesses
20 Access Programs Worldwide

Regional

[redacted]	Caracas	Havana	[redacted]	Kinshasa	Sofia	[redacted]	Berlin	[redacted]	Pristina	Guatemala City	[redacted]
[redacted]	Tegucigalpa	Panama City	[redacted]	Lusaka	[redacted]	Bangkok	[redacted]	[redacted]	Tirana	[redacted]	RESC
Geneva	Bogota	[redacted]	[redacted]	[redacted]	[redacted]	New Delhi	[redacted]	Phnom Penh	[redacted]	[redacted]	[redacted]
Athens	Mexico City	[redacted]	[redacted]	Budapest	[redacted]	[redacted]	Frankfurt	Sarajevo	[redacted]	[redacted]	Milan
Rome	Brasilia	[redacted]	[redacted]	Prague	[redacted]	Paris	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Quito	Managua	[redacted]	Lagos	Vienna	Rangoon	[redacted]	[redacted]	[redacted]	La Paz	[redacted]	Langley
San Jose	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Zagreb	[redacted]	[redacted]	Vienna Annex	Reston

FORNSAT

STELLAR	INDRA
SOUNDER	IRONSAND
SNICK	JACKKNIFE
MOONPEN	CARBOY
NY	TIMBERLIN
LADYLOVE	E



Bron: NSA

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

La nube es la computadora de otro

- La información se comparte con el proveedor:
  - Correos: Gmail, Hotmail, Yahoo, etc.
  - Voz/IP: Skype, Hangouts, etc.
  - Archivos: Google Drive, Onedrive, Dropbox

Dropbox mantuvo archivos eliminados por 7 años

itnews 26-Ene-2017

Twittear

Compartir

Dropbox ha admitido que "sin saberlo" ha mantenido los archivos y carpetas eliminadas en sus servidores durante siete años, culpando un error que impidió que dichos archivos fueran eliminados por completo.

http://www.seguridad.unam.mx/noticia/?noti=3146

creative commons

Europa mejora leyes de privacidad - GDPR

creative commons

https://privacidad.global/

Si no pagas por el servicio eres el producto

creative commons

https://privacidad.global/

Concentración de poder

Rank	Name	Company	Registered users	Active user accounts
1	Facebook	Facebook Inc.	2+ billion[3]	2.13 billion[4]
2	Facebook Messenger	Facebook Inc.	2+ billion[3]	1.3 billion[5]
3	WhatsApp	Facebook Inc.	1.5+ billion[6]	1.5 billion[6]
4	WowApp	Five River Inc.	1.5+ billion	1.5 billion[1]
5	WeChat	Tencent Holdings Limited	1+ billion[7]	1.0 billion[8]
6	Tencent QQ	Tencent Holdings Limited	1+ billion[9]	868 million[10]
7	Viber	Rakuten Inc.	900 million+[11]	900 million[11]
8	Instagram	Facebook Inc.	800+ million[12]	800 million[12]

creative commons

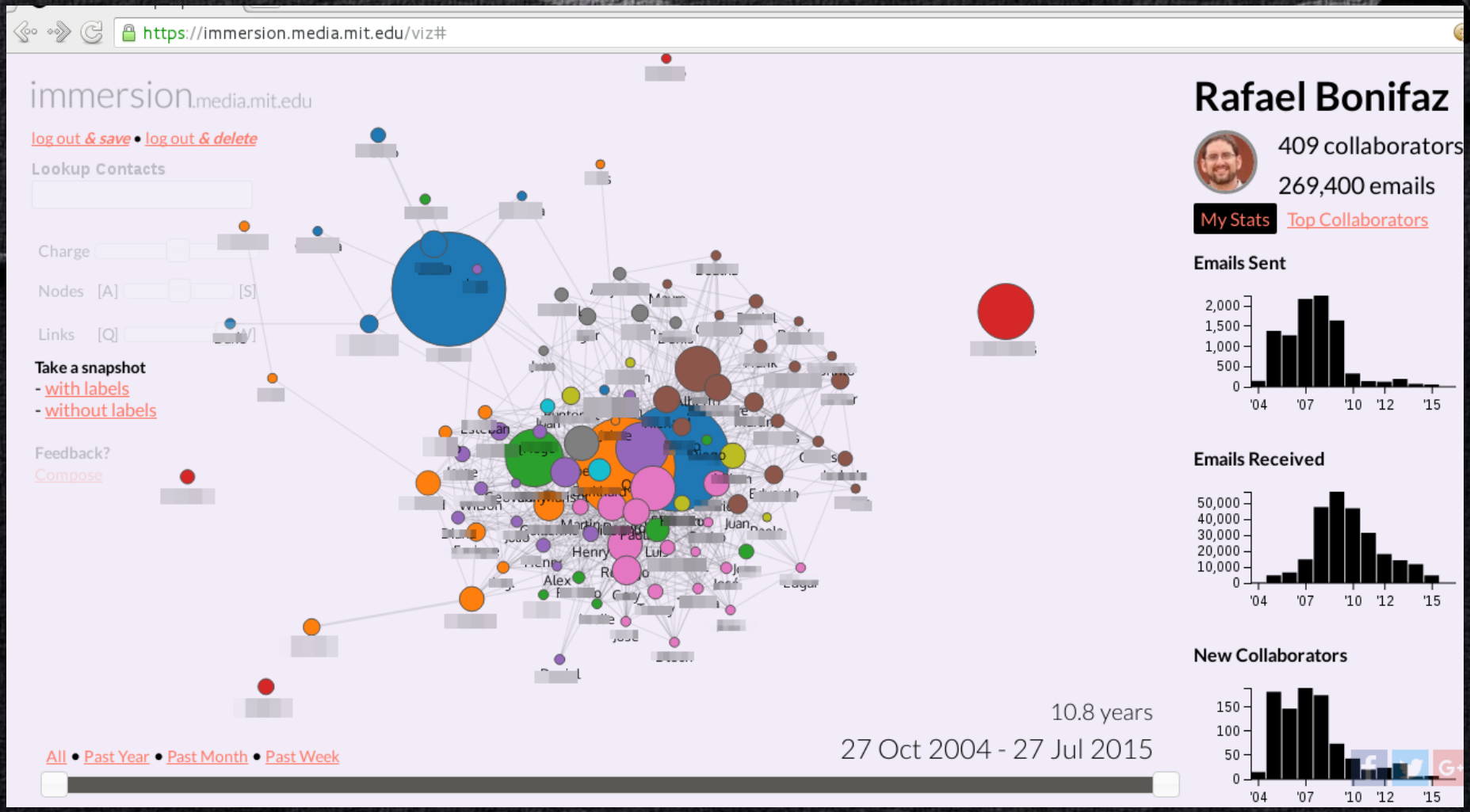
https://privacidad.global/

Datos y Metadatos

- Datos:
  - Contenido de las comunicaciones
  - El contenido de un correo
  - El audio de una llamada
  - Archivo digital
- Metadatos
  - Describen a los datos
  - Origen, destinatario, hora de un correo
  - Número de teléfono, ubicación geográfica
  - Nombre, tamaño, fecha de modificación de un archivo

creative commons

Metadatos



https://immersion.media.mit.edu/

creative commons

Ingredientes para la Privacidad

software libre, criptografía, anonimato, autonomía, comunidad, buenas costumbres y adaptabilidad al cambio

creative commons

https://privacidad.global/

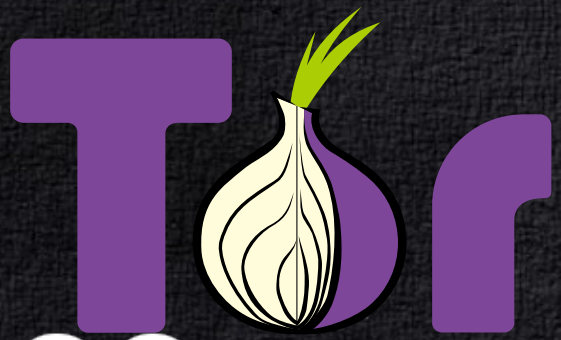
¿Qué es el Anonimato?

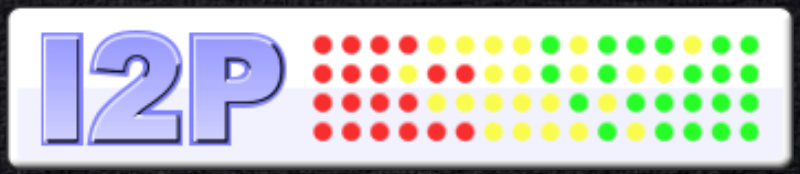
- Separar actividad identidad
- Ocultar metadatos

creative commons

Herramientas para Anonimato

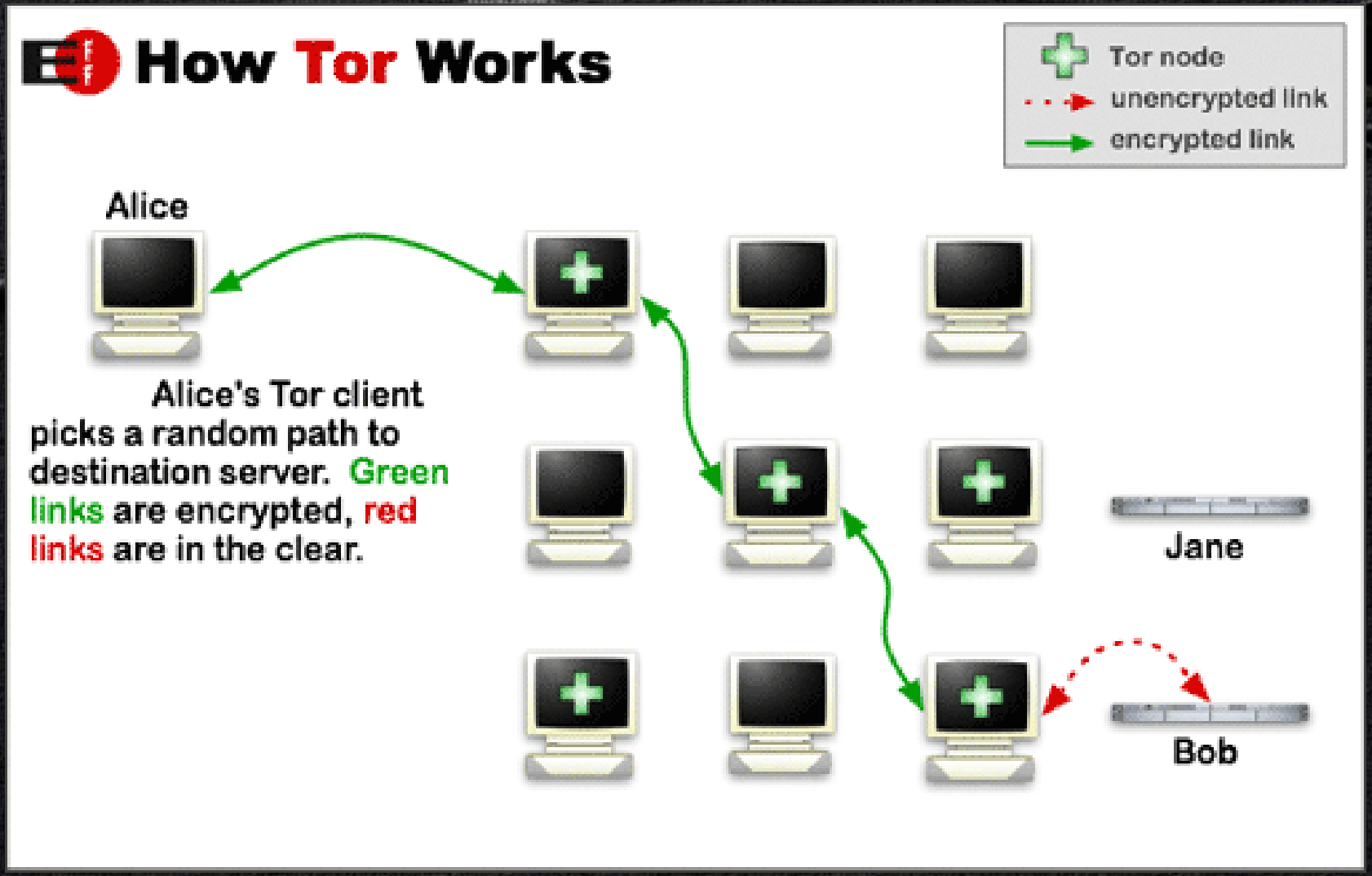
- VPN
  - Debes confiar en el proveedor de VPN
- Tor
  - Permite acceder a servicios TCP de manera anónima
  - Permite crear y acceder a servicios secretos TCP
- I2P
  - Permite crear y acceder a servicios secretos TCP/UDP





creative commons

Tor

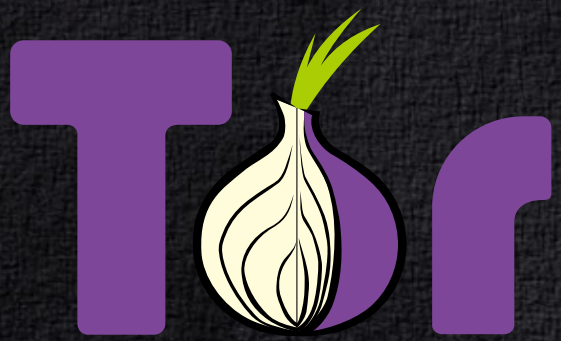


creative commons

https://privacidad.global/

Servicios ocultos de Tor o I2P

- Anonimato para el servidor
- Publicar servicios sin necesidad de IP pública
  - Accesibles solo a través de la red Tor o I2P
  - Tor soporta TCP, I2P TCP/UDP
- Autonomía en las comunicaciones



creative commons

Cifrado Extremo Extremo (e2e)

- Correo: OpenPGP
- Chat: OTR, Signal, XMPP/OMEMO, Wired, Matrix (OLM), Ricochet, Briar
- Voip: ZRTP

creative commons

Anonimato + Cifrado E2E

- Crear cuentas anónimas con Navegador Tor para correo, chat, ¿voz?
- Utilizar servicios ocultos para correo, chat y voz

creative commons

Correo Electrónico

- Crear cuenta anónima con Tor y acceder siempre con Tor
- Servicios como Protonmail, Tutanota o Mailfence permiten cifrar en navegador Tor
- Crear cuentas que soporten SMTP, POP3 e IMAP seguro
  - Acceder siempre con Tor (Torbirdy o Tails)
  - Cifrar siempre mensajes (GPG – Enigmail)
- Considerar seguridad sistema operativo y tipo de dispositivo
- Tails para mayor seguridad
- Servicio oculto para correo con Tor
  - ¿Servidor aislado o federado?
  - Direcciones del tipo alice@xstring7praro4.onion

creative commons

Chat

- Crear cuenta anónima desde el Navegador Tor o desde cliente a través de Tor
- Acceder a la cuenta siempre con Tor
- Utilizar cifrado e2e con OTR, OMEMO u otro
- Considerar seguridad sistema operativo y tipo de dispositivo
- Tails para mayor seguridad
- Servicio oculto para correo con Tor
  - ¿Servidor aislado o federado?
  - Direcciones del tipo alice@xstring7praro4.onion

creative commons

Voz / IP

- VoIP normalmente funciona sobre UDP por lo que no es soportado por Tor
- OnionCat permite publicar un servicio onion como IPv6 con suporte de TCP/UDP
  - Comunicaciones P2P (SIP/RTP)
- ¿Tox? ¿Ring?
- Mumble como servicio oculto de Tor
  - Mumble chat de voz que soporta TCP, consume poco ancho de banda y funciona bien con Tor

creative commons

Conclusiones

- Las comunicaciones en Internet están siendo almacenadas y vigiladas
- Comunicaciones Secretas (CS) son un ejercicio del Derecho a la Privacidad
- El software libre con criptografía permiten tener anonimato, secreto en comunicaciones y autonomía
- CS = Anonimato + Cifrado E2E + Buenas Costumbre
- Es posible que Alice pueda hablar con Bob sin que un tercero escuche/lea o incluso sepa que la conversación ocurrió
- Herramientas necesitan ser más amigables

creative commons

Una reflexión

“Si quieres construir un barco, no empieces por buscar madera, cortar tablas o distribuir el trabajo, sino que primero has de evocar en los hombres el anhelo de mar libre y ancho.”

Antoine de Saint-Exupéry

creative commons

Contacto

- Blog: https://rafael.bonifaz.ec
- Correo: rafael@bonifaz.ec
  38B8 6D44 6338 10DF 3334 204E CDFE 5731 6513 8A9F
- Mastodon: @rbonifaz@mastodon.social
- Twitter: @rbonifaz
- Privacidad Global: https://privacidad.global
  http://kbofqp5albsmiqqw.onion/
  @PrivacidadGlobal@mastodon.technology
  @PrivacidadGbl

creative commons