

Comunicaciones Seguras

Chat Seguro

Rafael Bonifaz: rafael@bonifaz.ec

Chat

- Permite tener una comunicación de una a uno o entre varios
- Requiere pocos recursos para la comunicación
- Permite enviar archivos multimedia
- Existen protocolos
 - IRC: Mensajería en grupo (salas de chat)
 - XMPP: Protocolo mensajería instantánea
- Ampliamente utilizado

#irc

Problemática del chat

- Si la información no viaje cifrada podría ser espiada
- Es posible el robo de identidad
- Es vulnerable al ataque del hombre en el medio
- Mayoría de gente utiliza servicios “gratuitos” de alguna empresa grande Internet
- Muchas de estas empresas colaboran con la NSA
- Servicios como WhatsApp, Telegram o Signal se basan en servicios centralizados

NSA

TOP SECRET//SI//ORCON//NOFORN

msn Hotmail® Google™ skype® paltalk.com. YouTube AOL mail

Gmail™ facebook

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

Current Providers

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

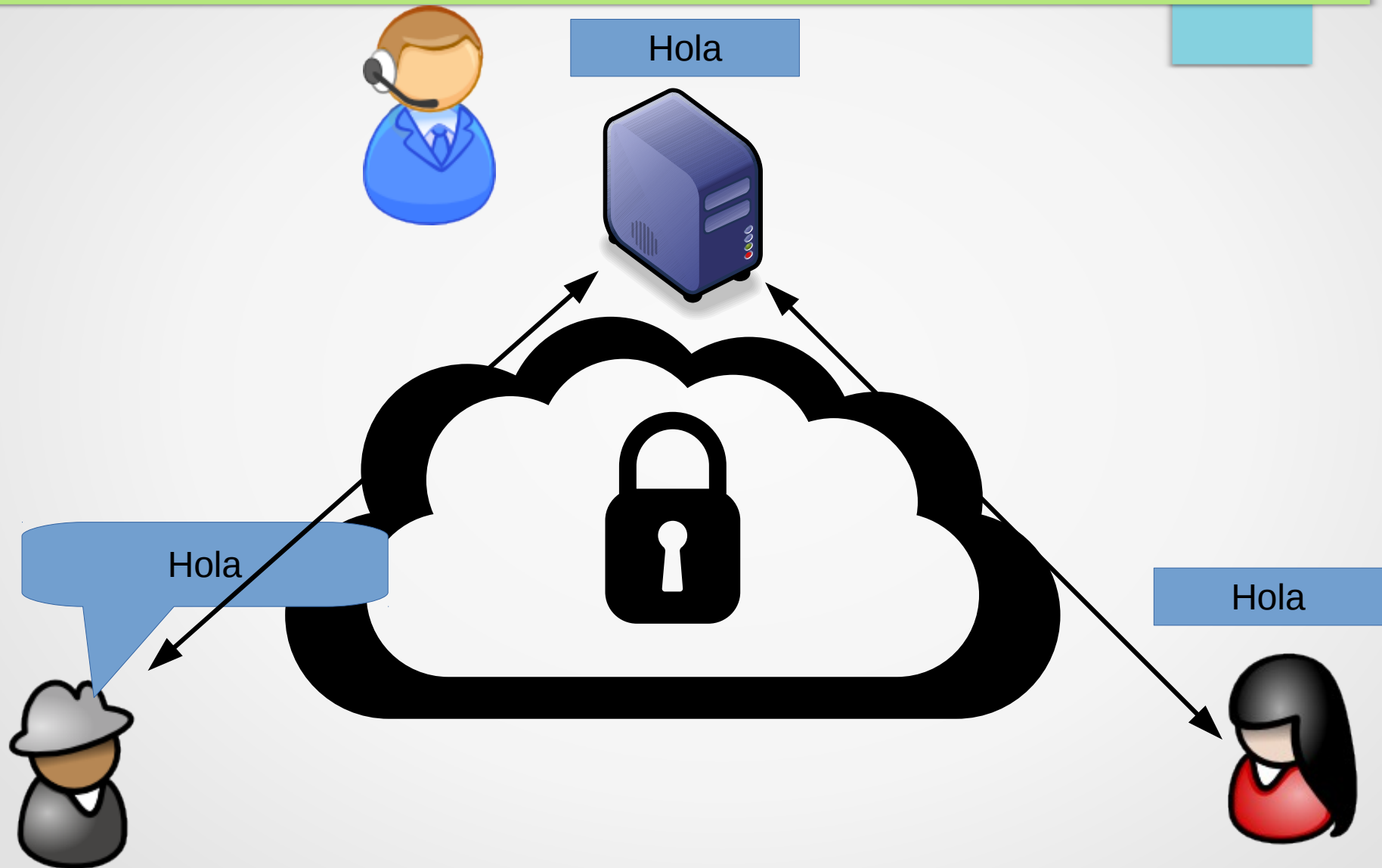
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

- 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

TOP SECRET//SI//ORCON//NOFORN

Cifrado entre cliente y servidor



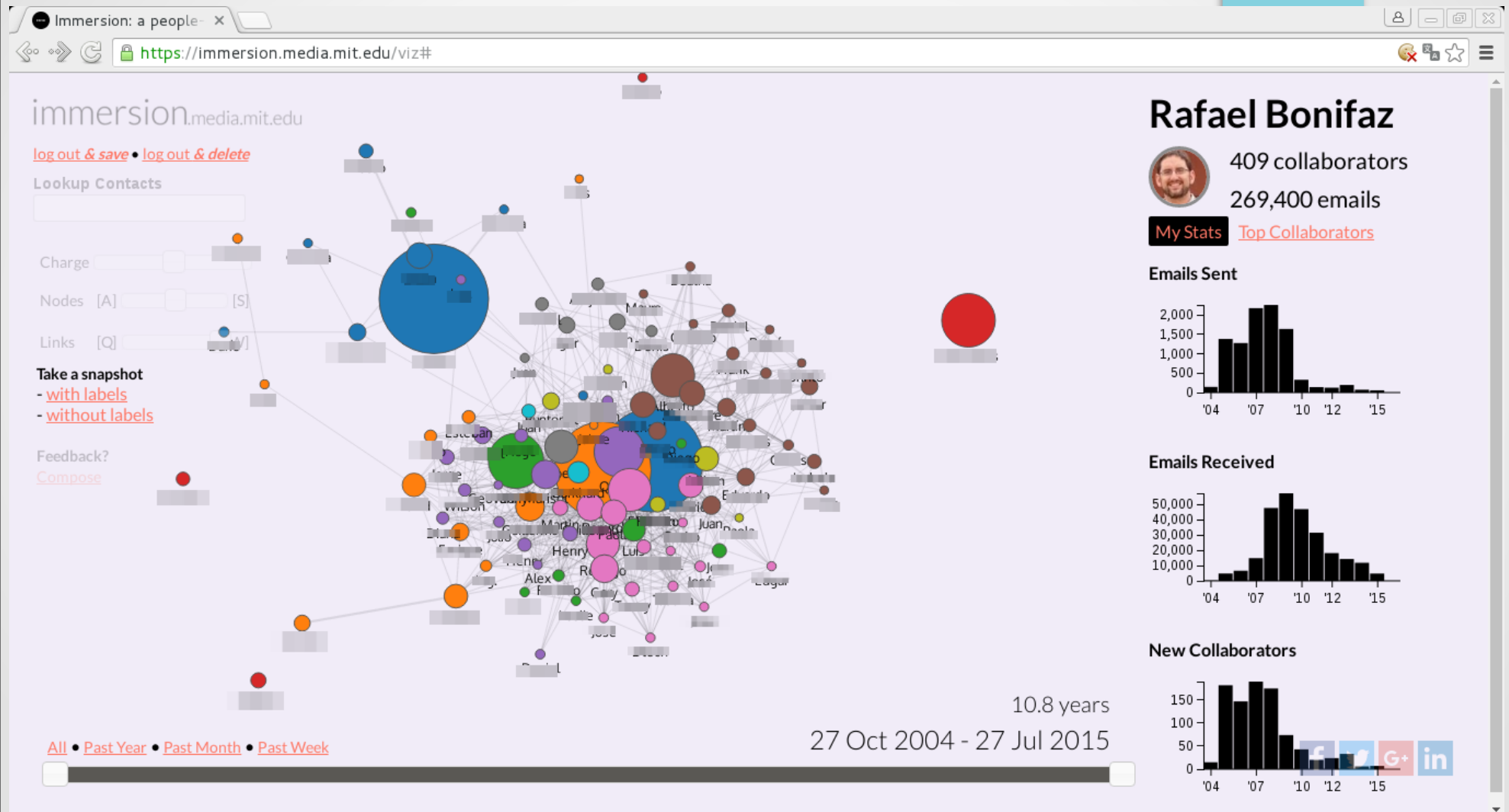
Cifrado fin a fin



Metadatos

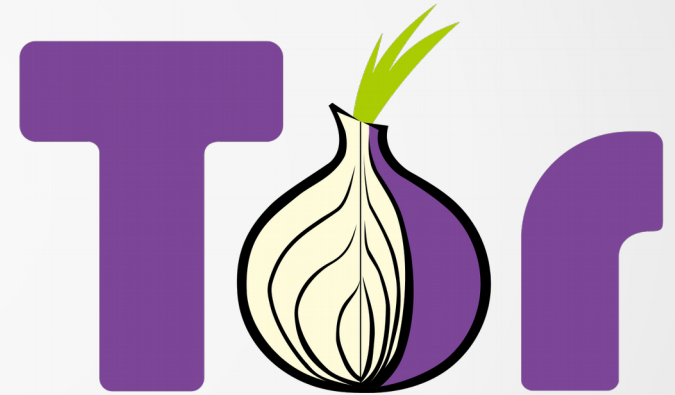
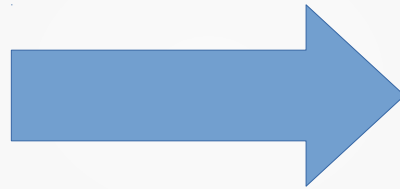
- Datos sobre los datos
- ¿Quién se comunica con quién?
- ¿Con qué frecuencia?
- ¿Cifra o no cifra la comunicación?
- ¿Ubicación geográfica?
- Los metadatos se pueden ocultar con Tor

Metadatos



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

Tor permite ocultar metadatos

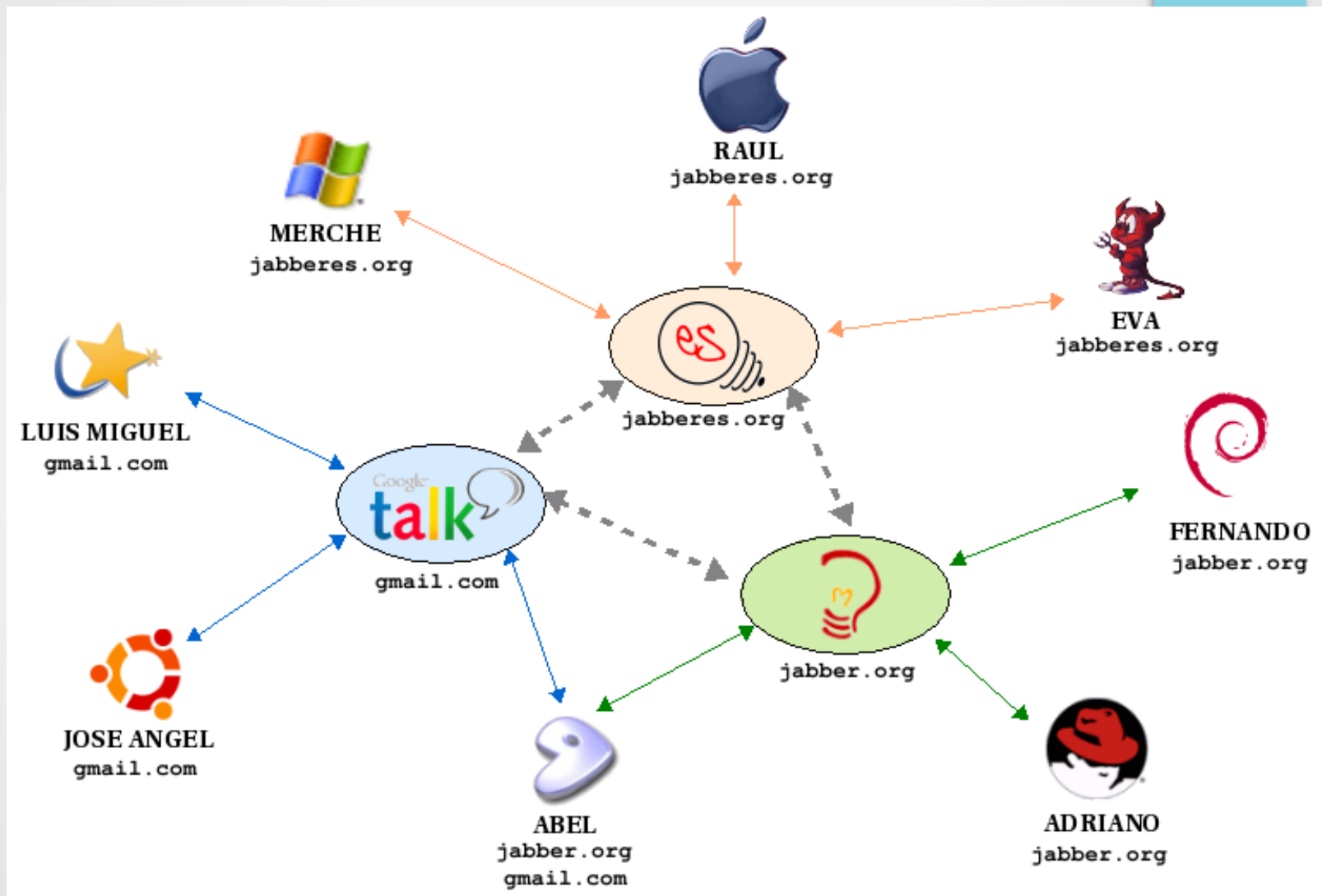


Protocolo XMPP

- Protocolo estándar de chat creado en 1999
 - <http://www.xmpp.org/>
- Protocolo federado similar al correo electrónico
- Varios servidores
 - Jabberd, Ejabberd, Openfire, Prosody, etc.
- Varios clientes
 - Pidgin, Adium, Conversations, Tor Messenger
- Es protocolo extensible
 - Puede soportar Voz/Ip
- Listado de servidores
 - <https://xmpp.net/directory.php>
 - <https://www.jabberes.org/servidores>



Protocolo XMPP



<https://www.jabberes.org/introduccion>

Protocolo OTR

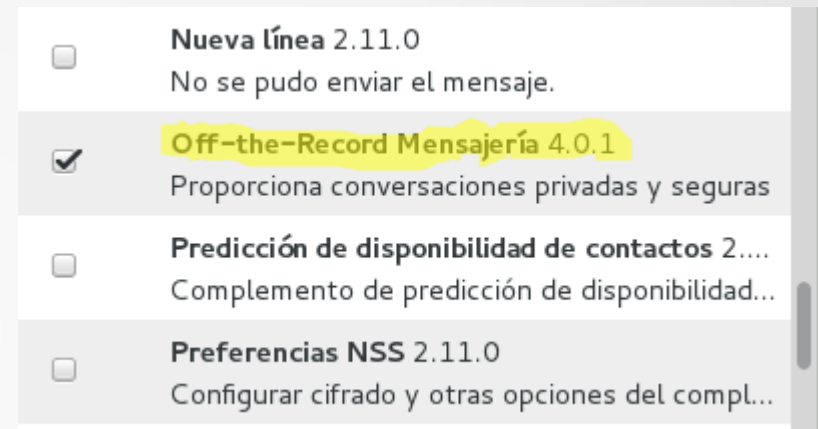
- *Off The Record* (fuera de Registro)
- Protocolo para asegurar comunicaciones de chat fin a fin
 - Confidencialidad
 - Autenticación
 - Repudio (Off the record)
 - *Perfect forward secrecy*
- Intercambio de clave: Diffie Hellman
- Cifrado de mensaje: AES
- Autenticación con llaves públicas a través de DSA
 - Verificación manual de fingerprints
 - Pregunta respuesta

Cifrado fin a fin



Configurar OTR en Pidgin

- Pidgin es un cliente multiprotocolo y multiplataforma (Adium en Mac)
- Utiliza libpurple como backend
- Por defecto no trabaja con OTR
- Se debe instalar el plugin
- En distribuciones basadas en Debian se instala pidgin-otr y pidgin-otr
- Se debe configurar OTR manualmente
- Pidgin y OTR funciona para XMPP y otros protocolos



Configurar Tor en Pidgin

- Se puede configurar a través de ProxySocks
 - Puerto 9050 si se usa el servicio Tor
 - Puerto 9150 si se usa Navegador Tor
- Otra opción es usar **torsocks**

```
$ torsocks pidgin
```

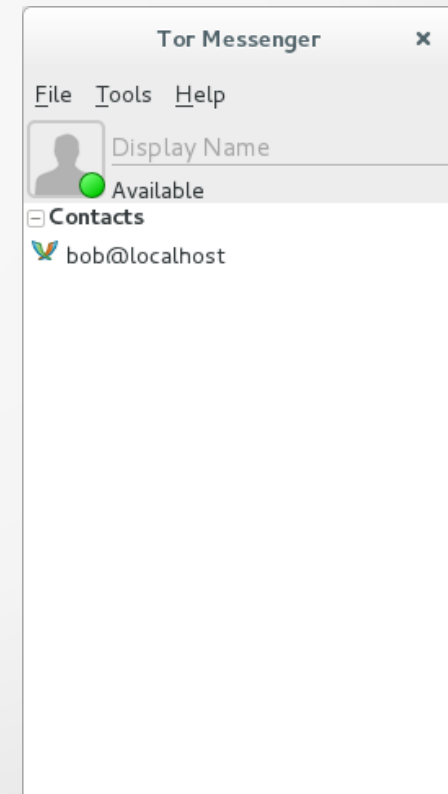
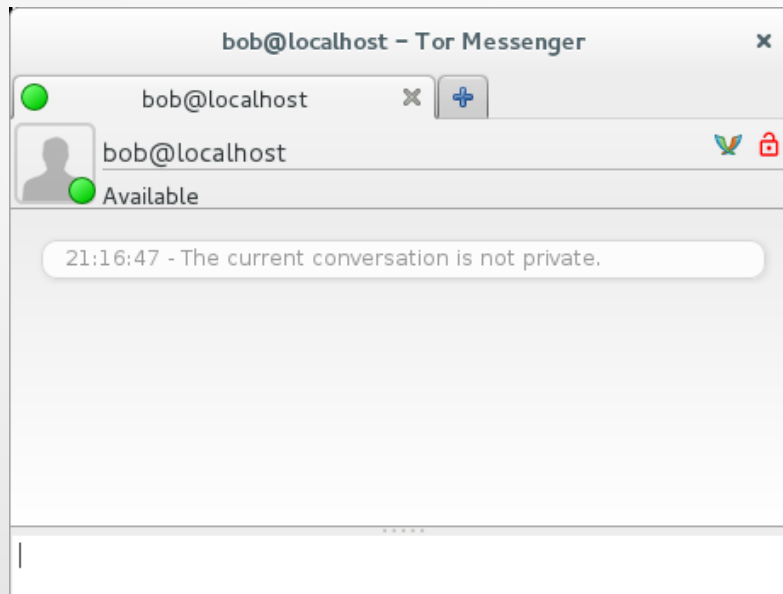


The screenshot shows the 'Modificar cuenta' (Modify account) dialog box in Pidgin, with the 'Pasarela' (Gateway) tab selected. The dialog has four tabs: 'Básica', 'Avanzadas', 'Pasarela', and 'Voz y vídeo'. The 'Pasarela' tab contains the following fields:

- Tipo de proxy: SOCKS 5 (dropdown menu)
- Servidor: localhost (text input)
- Puerto: 9050 (text input)
- Nombre de usuario: (empty text input)
- Contraseña: (empty password input)

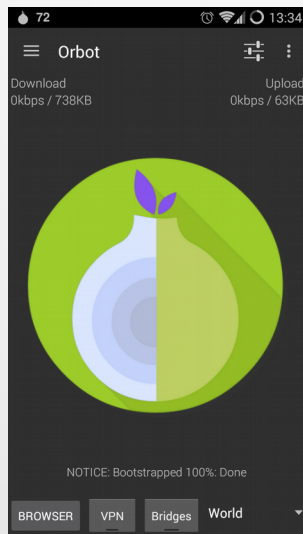
Tor messenger

- Funciona con XMPP y otros protocolos
- Viene con su propio servicio de Tor embebido
 - Similar al navegador Tor
- OTR preconfigurado



OTR en Celular

- Conversations
 - Disponible en Fdroid
 - Disponible mediante pago en Google Play
- Se puede combinar con Orbot (Tor)



← Añadir cuenta

Identificador Jabber 1
bob@localhost

Contraseña 2
.....

Hostname 3 Puerto
mfg75grfpgr2763r.onion 5222

☐ Registrar nueva cuenta en servidor

Cancelar | Siguiete 4

Autenticar usuarios

- Una sesión OTR cifra automáticamente sin validar usuarios
- Una vez validado el canal se autentican los usuarios
- Se lo puede hacer mediante pregunta – respuesta, secreto compartido o manual
- La autenticación se hace una sola vez
- Sirve para evitar suplantación de identidad y ataque de *man in the middle*

Man in the Middle

