

TOOL



NOW IT'S
YOUR TURN.

Secure Messaging Scorecard

- L'Electronic Frontier Foundation (una ONLUS che dal 1990 si occupa di privacy, libertà di espressione, innovazione, etc..) ha stilato una lista di software per la messaggistica istantanea, valutando alcune componenti particolarmente importanti per la privacy.
- I criteri di valutazione sono stati i seguenti:
Cifratura del traffico, cifratura end 2 end, autenticità della comunicazione, auditing del software, documentazione adeguata, etc..

<https://www.eff.org/secure-messaging-scorecard>

Featured Tools ▼	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM							
CryptoCat							
Facebook chat							
Google Hangouts/Chat "off the record"							
iMessage							
Jitsi + Ostel							
Off-The-Record Messaging for Mac (Adium)							
Off-The-Record Messaging for Windows							

Per ogni strumento vedremo:

- A cosa mi serve? Cosa mi offre?
- Come si colloca nel threat model?
- Come si installa
- Come si usa
- Come funziona
- Install fest! =)

The screenshot shows a text editor window titled "mein öffentlicher Schlüssel - Nachricht (Nur-Text)". The editor contains a GPG public key block starting with "-----BEGIN PGP PUBLIC KEY BLOCK-----" and ending with "-----END PGP PUBLIC KEY BLOCK-----". The key is for "adele@gnupp.de".

Overlaid on the right side of the text editor is the "Gpg4win Setup" window. It features the GPG logo and a large yellow padlock with the word "GPG" on it. The window title is "Gpg4win Setup" and the subtitle is "Completing Wizard". There are buttons for "Click Finish to close" and "Click here for the" (partially visible). A checkbox labeled "Show the RE" (partially visible) is also present.

Cosa mi offre?

- Confidenzialità: cifra file ed email.
- Autenticità
- Integrità
- Uno dei sistemi crittografici più forti e usati al mondo!

Da chi mi protegge?



Come si installa, come si usa?

- Andiamo a fare un salto su:
<http://www.deepdotweb.com/2015/02/21/pgp-tutorial-for-windows-kleopatra-gpg4win/>
?



Case scenario

- Email di lavoro
- Non vuoi che gmail sappia cosa dici/cosa ti piace/chi sei
- Dati medici sul proprio computer
- Foto “allegre” ? :)
- Chiavette, dischi esterni
- Dropbox e altri cloud
- ...

OSX?



GPG Suite

Everything you need to get started with secure communication and encrypting files in one simple package.

Use GPG Suite to encrypt, decrypt, sign and verify files or messages. Manage your GPG Keychain with a few simple clicks and experience the full power of GPG easier than ever before.

For OS X 10.10 Yosemite

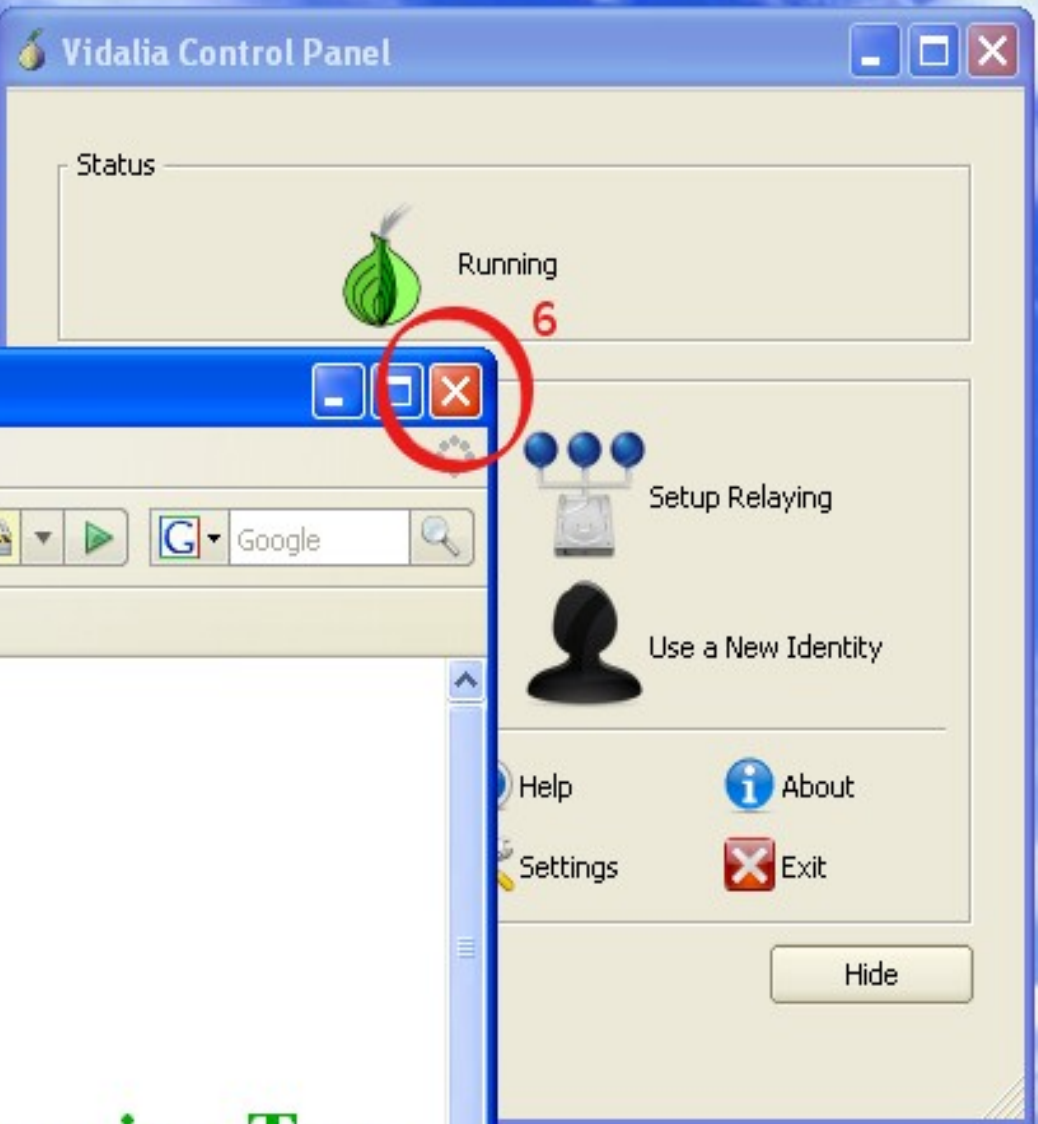
Compatible back to OS X 10.6



Download GPG Suite

```
>install
```

```
>fest_
```

Da chi/cosa mi protegge?

Privacy: SI

Anonimità: SI

Navigazione: SI

Mail: No

Confidenzialità: Forse...

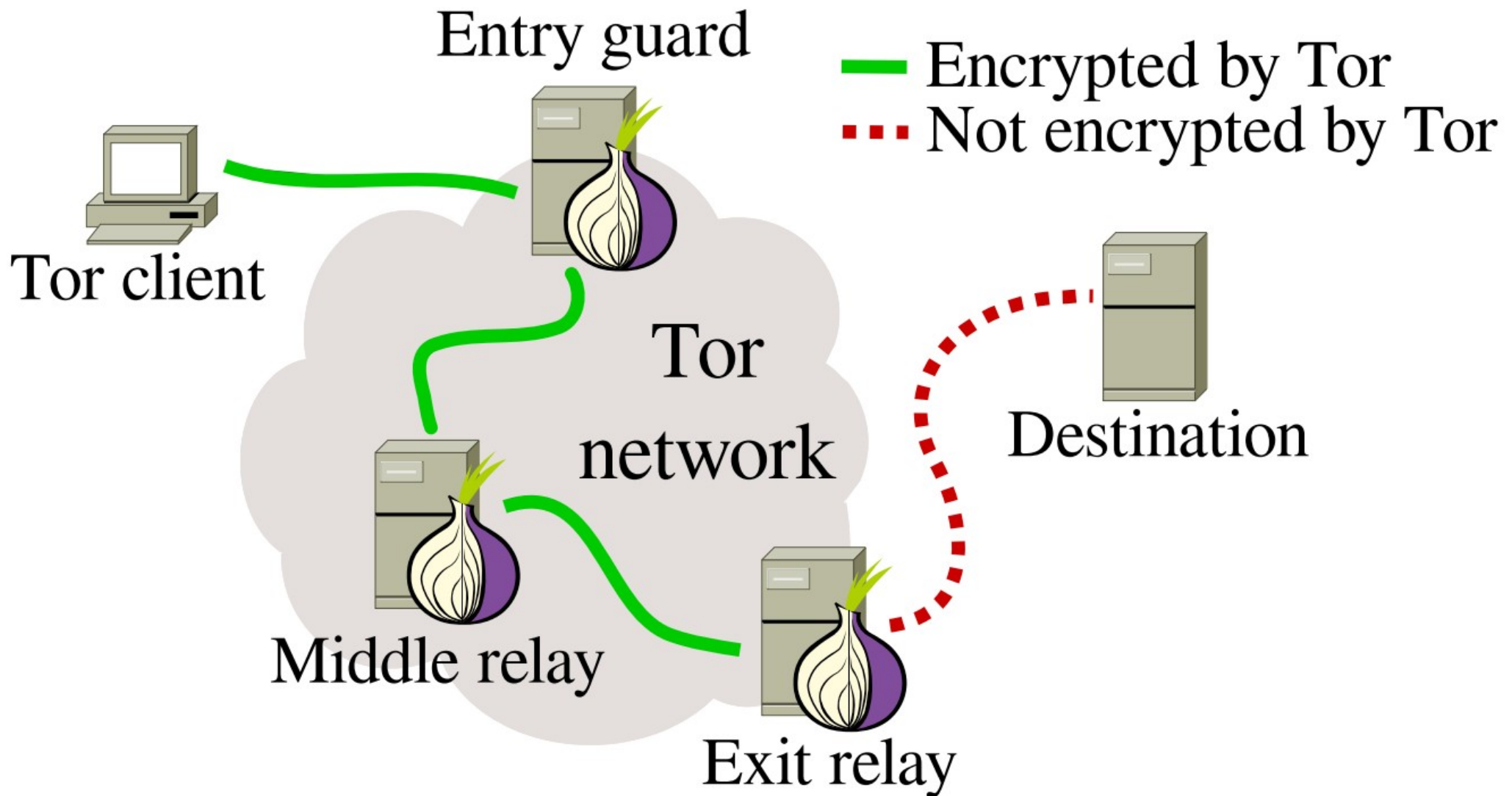
Come si installa?

- Si installa? No! Si scarica!
- <https://www.torproject.org/download/download>

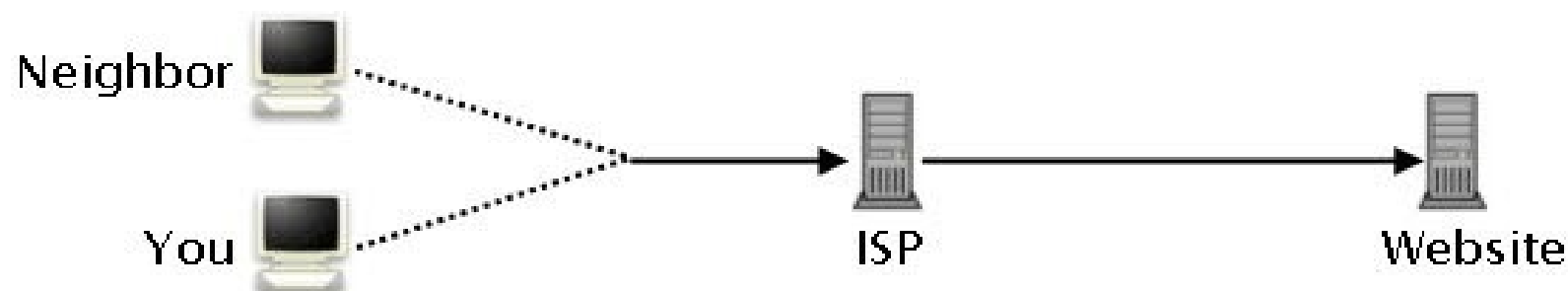
Come si usa

- Come un normalissimo browser..
- Con alcune accortezze: cerchiamo sempre siti “https”, e non divulghiamo i nostri dati sensibili.

Come funziona?



Come funziona



NORMAL DIRECT CONNECTION



..... Wireless — Normal — Encrypted

ENCRYPTED ANONYMOUS CONNECTION

MEGALEECHER.NET

Case scenario

DarkWeb, tor2web

- “Tor is a software project that lets you anonymously browse the Internet. Tor2web is a project to let Internet users access anonymous servers.”

```
>install1  
>fest_
```

RedPhone

RedPhone
security, simplified.



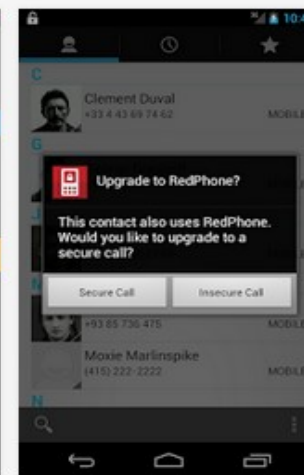
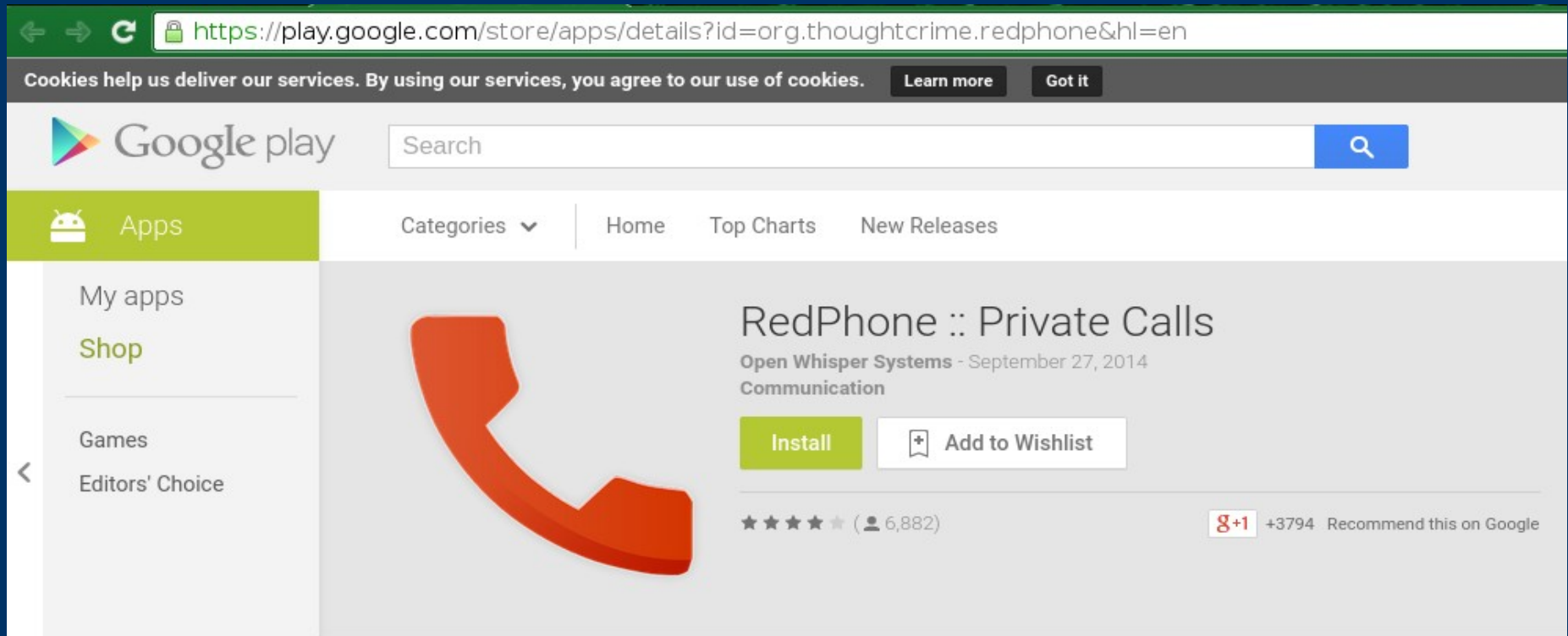
<https://whispersystems.org>

VicinoLontano 2015

Da chi/cosa mi protegge?

- Confidenzialità
- Autenticità
- Intercettazione telefonica fatta da praticamente chiunque.

Come si installa?



Come si usa

- Dobbiamo registrarci: diamo il nostro numero e la nostra rubrica a WhisperSystem (poco anonimo...)
- Una volta registrati, possiamo chiamare solo chi ha redphone

Come funziona?

iOS?

Signal - Private Messenger

[View More by This Developer](#)

By Open Whisper Systems

Open iTunes to buy and download apps.



Description

Privacy is possible. Signal makes it easy.

* Say Anything - Send high-quality group, text, picture, and video messages, all without SMS and MMS fees.

[Open Whisper Systems Web Site](#) ▶ [Signal - Private Messenger Support](#) ▶

[...More](#)

What's New in Version 2.0.3

Fixes critical bug with push notifications for new users.

TextSecure

The image shows the Google Play Store page for the app "TextSecure Private Messenger". The page header includes the Google Play logo, a search bar, and navigation tabs for "Apps", "Categories", "Home", "Top Charts", and "New Releases". On the left, a sidebar lists "My apps", "Shop", "Games", and "Editors' Choice". The main content area features the app's icon (a blue speech bubble with a white keyhole), the title "TextSecure Private Messenger", the developer "Open Whisper Systems" (dated May 6, 2015), and the category "Communication". Below this are "Install" and "Add to Wishlist" buttons. The app has a 4.5-star rating from 17,232 reviews and a "g+1" badge with "+6590 Recommend this on Google". At the bottom, four preview images show the app's interface: a conversation with "Masha Kolenkina", a list of contacts, a "New group" screen for the "Nihilist History Book Club", and a screen with a green keyhole icon and a passphrase input field.

Google play Search

Apps Categories Home Top Charts New Releases

My apps Shop Games Editors' Choice

TextSecure Private Messenger

Open Whisper Systems - May 6, 2015
Communication

Install Add to Wishlist

★★★★☆ (17,232) g+1 +6590 Recommend this on Google

Preview images showing the app interface:

- Conversation with Masha Kolenkina (415) 266-1888.
- TextSecure app interface showing a list of contacts.
- New group interface for Nihilist History Book Club.
- TextSecure app interface showing a green keyhole icon and a passphrase input field.

VicinoLontano 2015

Cose Offre?

- Sviluppato da WhisperSystem, offre il corrispettivo di RedPhone per sistemi Android: cifratura per messaggistica istantanea. E' compatibile con Signal (iOS).

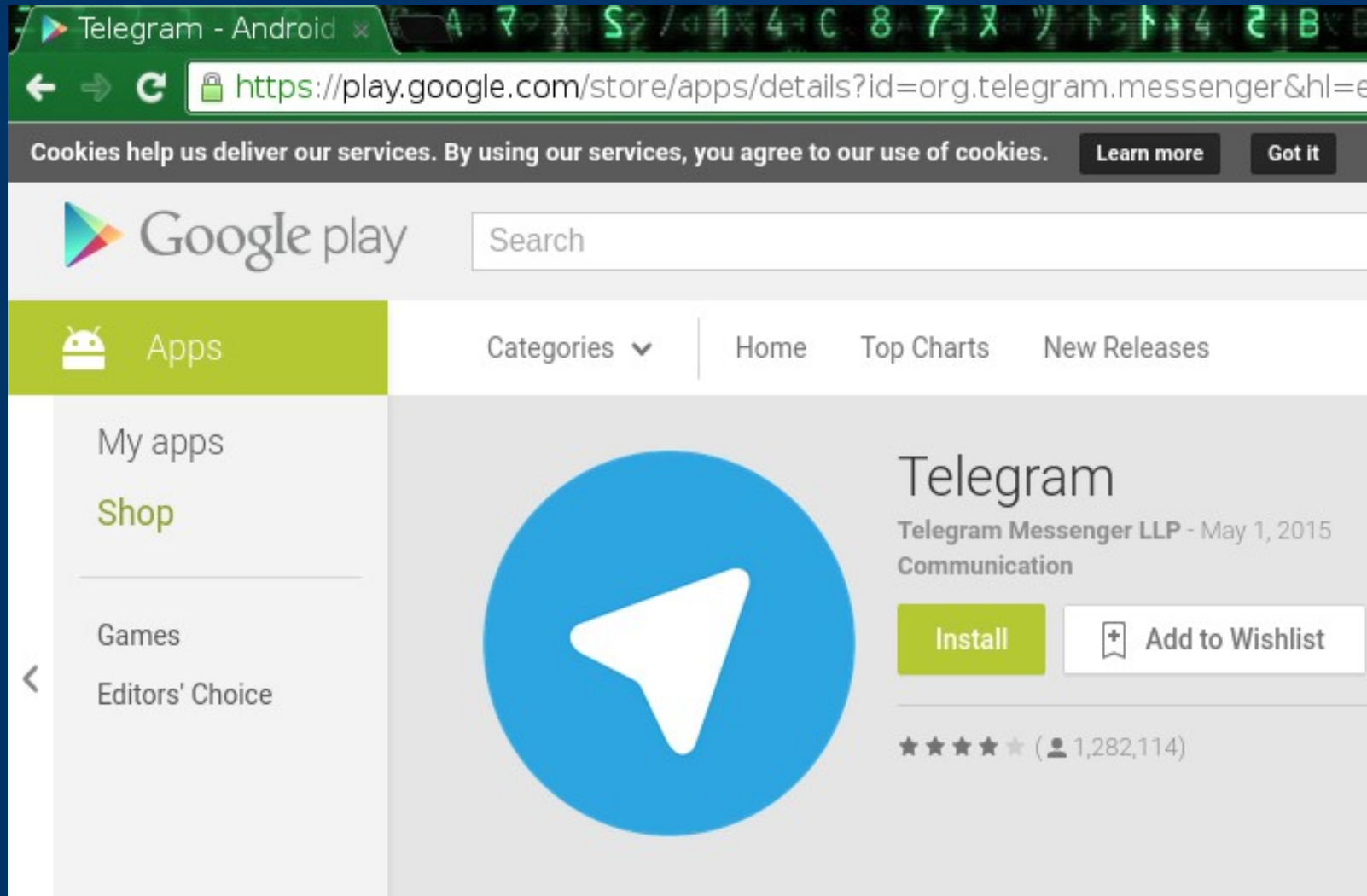
```
>install
```

```
>fest_
```

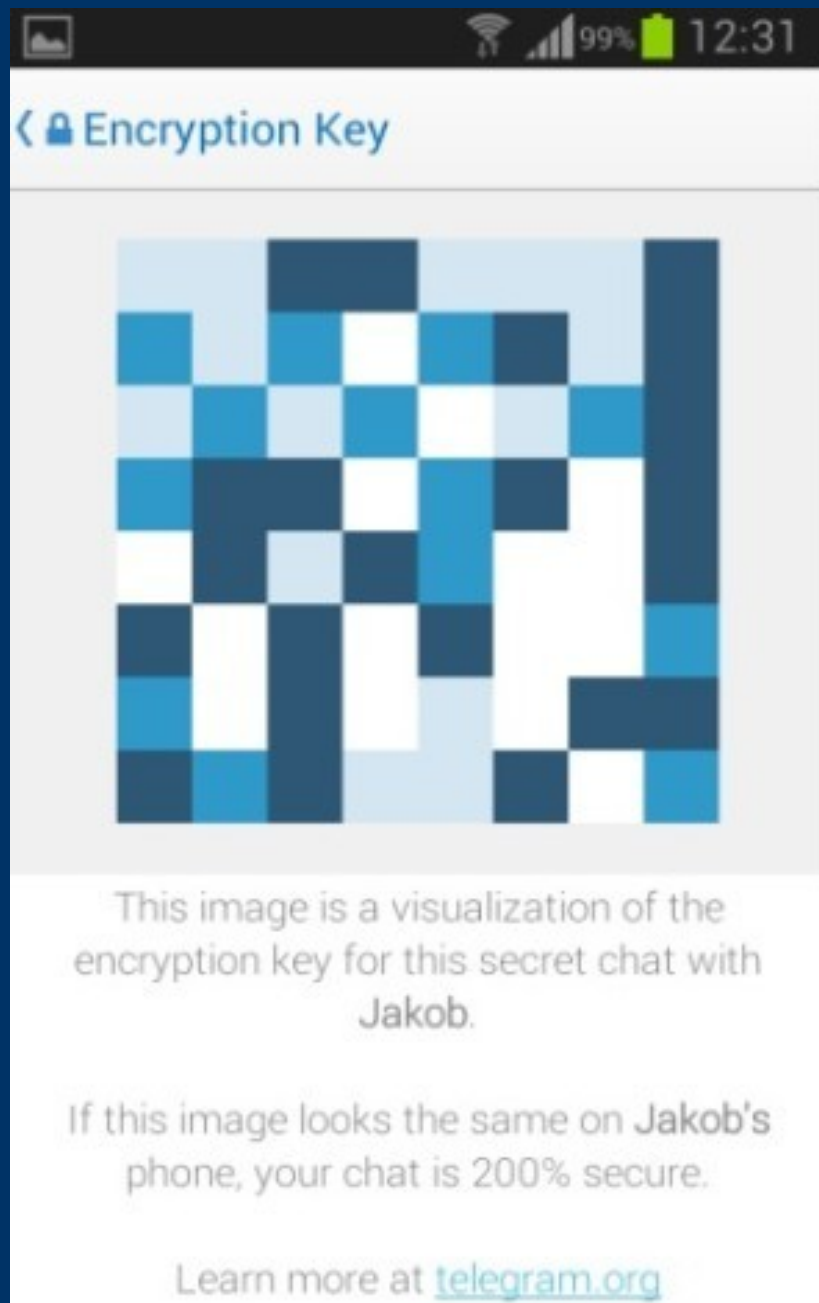
Telegram



Come si installa?



Come si usa?



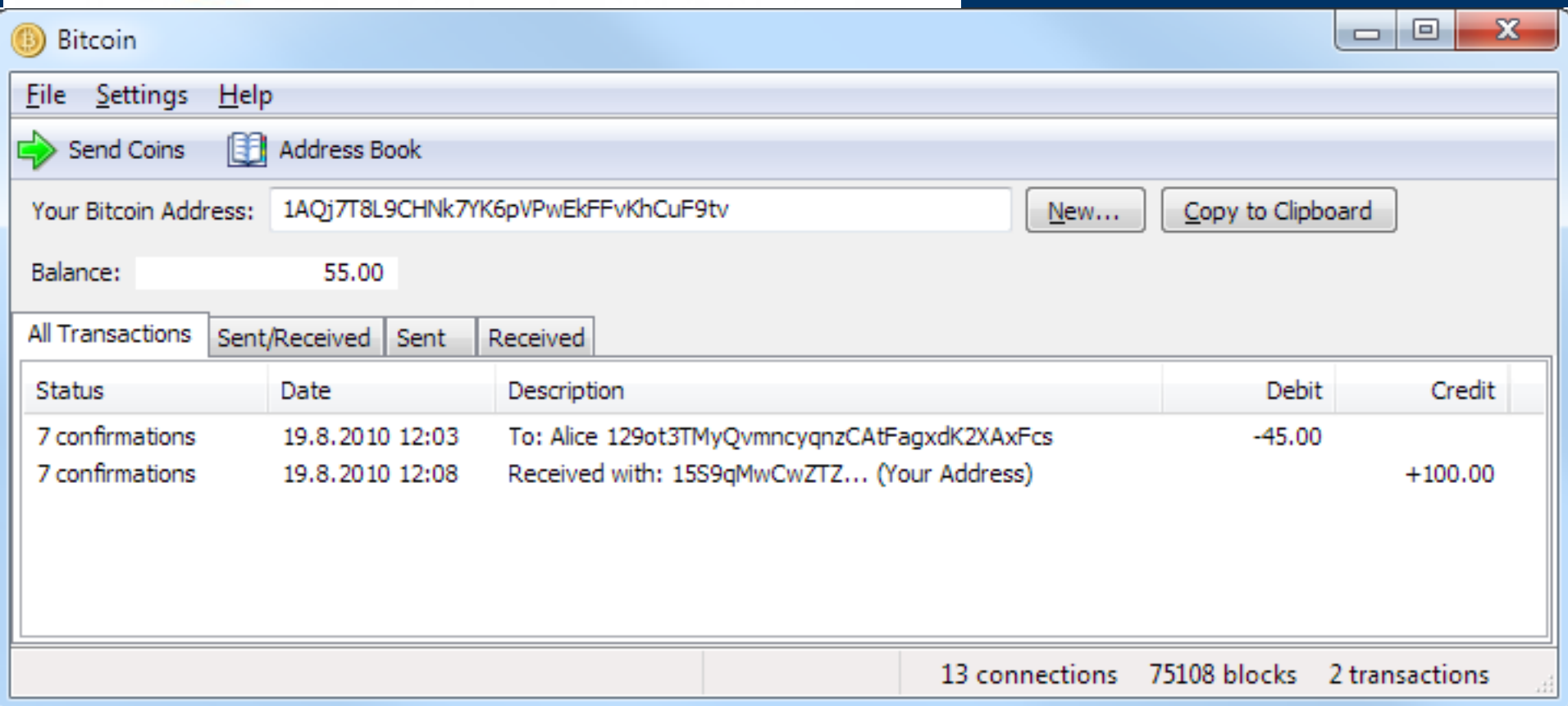
Case scenario

Perfetto per le amanti :P



```
>install1  
>fest_
```

Bitcoin e crittomonete



[Send Bitcoins](#)[Receive Bitcoins](#)[Wallet Properties](#)[Offline Transactions](#)

Armory 0.87-beta / Expert User

Available Wallets:[Create New Wallet](#)[Import Wallet](#)

ID	Name	Security	Balance
9jCTtF1H	What What	Encrypted	(...)

[Dashboard](#)[Transactions](#)**Armory is offline while scanning the blockchain****Please be patient, scanning may take several minutes!**

Armory will go into online mode automatically, as soon as the scan is complete.

The following functionality is available while scanning in offline mode:

- Create new wallets
- Generate receiving addresses for your wallets
- Create backups of your wallets (printed or digital)
- Change wallet encryption settings
- Sign transactions created from an online system
- Sign messages

NOTE: The Bitcoin network will process transactions to your addresses, regardless of whether you are online. It is perfectly okay to

Cosa/Dove posso comprare?

- QuiBitcoin
- Online Markets
- Bitcoin exchange

Tunnel Cifrati

<https://mullvad.net/en/>

Compatibile con iOS, Android,
OSX, Linux, Windows!



Cosa proteggono?

- Confidenzialità
- Integrità
- Autenticità

Case scenario



