

Computer Security 101



A CRASH COURSE

a hackbloc initiative

Who is Hackbloc?

Our mission is to research, create and disseminate information, tools, and tactics that empower people to use technology in a way that is liberating. We support and strengthen our local communities through education and action. We strive to learn from each other and focus our skills toward creative goals, to explore and research positive hacktivism, and to defend a free internet and free society!



staff{at}hackbloc.org

exploit code not people

Setting Up A Security Process

• *Identify risks + adversaries*

Possible Risks:

- › Lawsuits
- › Smear campaigns
- › Jail time
- › Job/financial loss
- › Court orders/censorship
- › Excommunication
- › Physical harm
- › Death

Possible Adversaries:

- › A company
- › Your boss
- › The cops
- › The public
- › A group of other people
- › A hell-bent crazy person
- › The media



It's about information control

Security Theory

- *Security = (Time + Effort)/(A's Time + A's Effort)*
- *Security is insured by technology and trust*



only a fool believes they are secure

Rules of Thumb

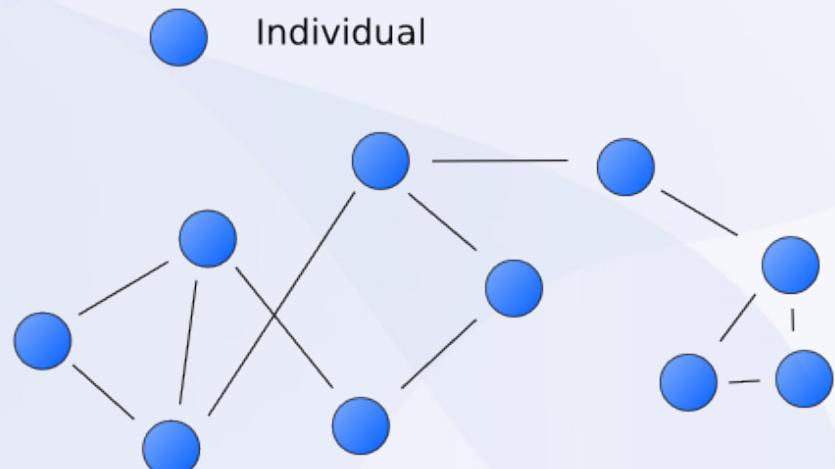
- *The house only has to win once*
- *Security always fails*
- *Security through obscurity isn't*
- *Defense in-depth*
- *As good as those who implement it*
- *Be realistic*
- *Security favors minimalism*
- *Use common sense*



think for yourself

Security Culture

- *Is a set of social standards for protecting a social network from adversaries*
- *Controls information*
- *Is a lie*
- *Is a tool*



only a fool believes their friend is secure

Security Culture Cont

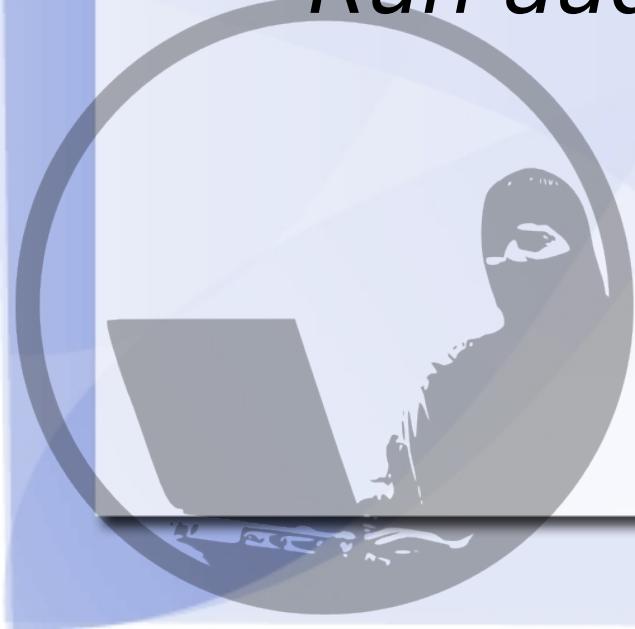
- *Do not share people's info without permission (phone # example)*
- *CC vs BCC on email*
- *Make a network map!*
- *Don't leave contact lists laying around, applies to mailing lists too*



only a fool believes their friend is secure

Implementing Security Process

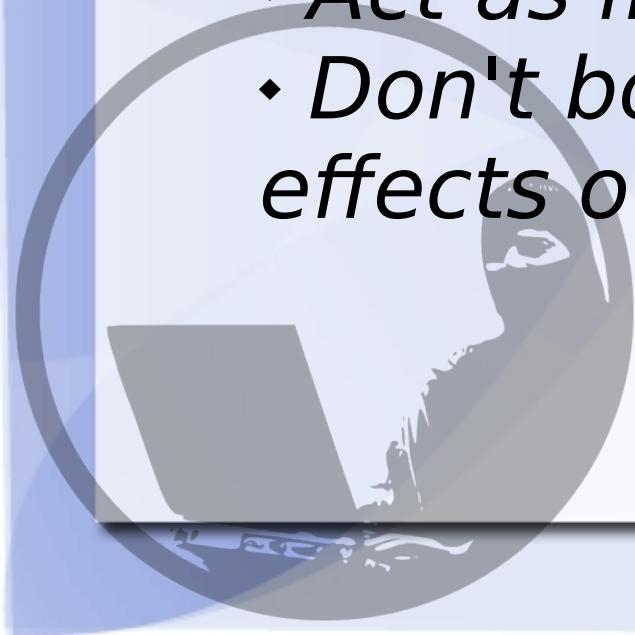
- *Call out others, yourself*
- *Lead through example*
- *Mistakes shouldn't be embarrassing*
- *Be honest when you make a mistake*
- *Run audits*



only a fool believes they are secure

Personal Security

- *Make personal security policy*
- *The higher your risks, the lower your profile should be*
- *Don't be intimidated by surveillance*
- *Act as if raid is always coming*
- *Don't bottle up psychological effects of surveillance*



only a fool believes they are secure

Choosing Who to Work With

- *Do you need to be careful about who you ask?*
- *Gradually increase risk*
- *Consider their risk profile*
- *How do they handle stress? Are they reliable? Do they have an addiction?*
- *Why do they want to be involved? Will that reason change?*



Secure Communications

- *Be careful what you say over all mediums, especially electronic ones*
 - *Check who is listening*
 - *Don't use codewords*
 - *Chatter & Network Analysis*
 - *If they're not involved, they shouldn't be party to your conversation*



only a fool believes they are secure

Rumor Control

- *Verify stories and statements*
- *Don't spread information you don't know to be true*
- *Fight snitch jacketing*



only a fool believes they are secure

Publishing Anonymously

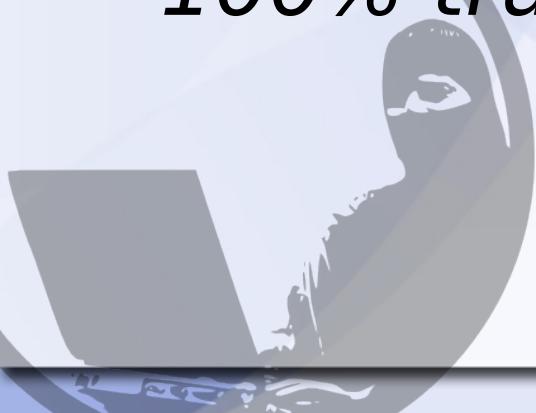
- *Noise signatures, EXIF data*
- *Compromising formats (PDF, etc)*
- *Yellow dots*
- *Where are you publishing from?*
- *Who are you publishing to?*



only a fool believes they are secure

Dealing with Media

- *Plan out what they're going to ask*
- *Classic infiltration strategy, be wary of requests to meet “direct activists” or be “embedded”*
- *Research the interviewer, demand credentials*
- *No reason to use real name or be 100% truthful*



Bugs and Eavesdropping

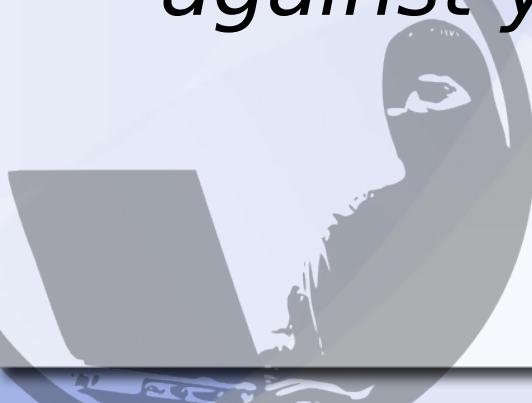
- *Audio, laser, electronic, directional mics*
 - *Design of bug tells you intent, ownership*
 - *Bugs need a power source and way to transmit information*



only a fool believes they are secure

Things to look out for

- *Keep log of suspicious activity*
- *Delayed/opened mail*
- *Sudden influx of new members*
- *Quickly changing attitude/personality/behaviour*
- *Show-off/bragging behaviour*
- *Not all parts of state are working against you in synchronized fashion*



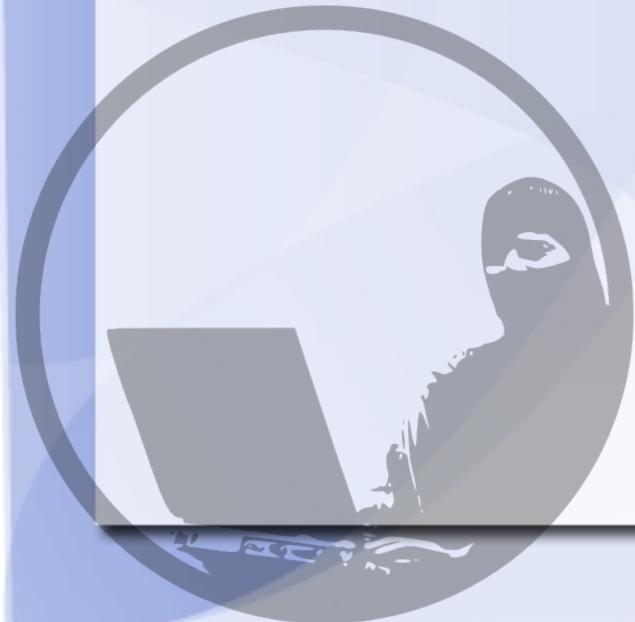
Preventing Infiltration

- *Get to know members personally*
- *Make cover stories expensive*
- *Infiltrators vs paid informants*
- *Not only militant groups targeted*
- *Inexperience doesn't = snitch*
- *Don't generate paranoia culture*



Do you have an infiltrator?

- *Campaign problems, moves anticipated*
- *Opponent's history/resources*
- *Inconsistent stories*
- *Attempts to get information*
- *Internal disruption*



Gathering evidence

- *Talk to a lawyer*
- *Do damage control*
- *Keep notes*
- *Probe suspect + check references*
- *Consider surveillance + searches*
- *Setup opportunities for self-incrimination*



Final Steps

- *Pics or it didn't happen*
- *Present the accusation w/ evidence*
- *Keep end goal in mind*
- *Who needs to know?*
- *Discuss incident w/ group*
- *Stress people not become paranoid*
- *Revise security policies*

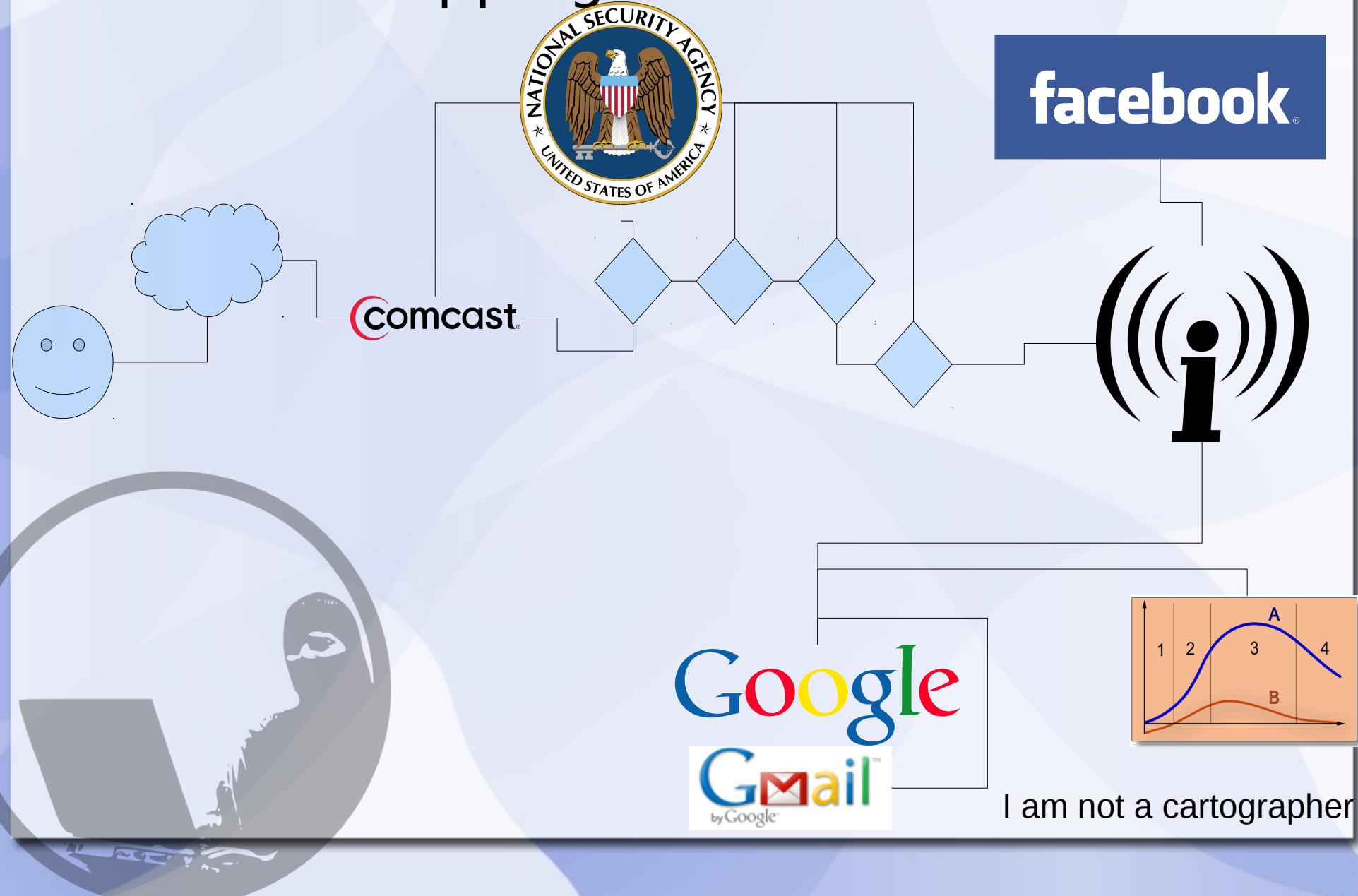


Post-Action Analysis

- *Look for separation/special treatment*
- *Look for police citing specific evidence*
- *Make arrest policy clear*
- *Support arrestees as security culture*



Mapping Data Transfer





Long Haul 2008

The Long Haul Infoshop, a community center/library in Berkeley was raided by the FBI and local police. Over a dozen computers were seized in addition to check-out logs because a threatening email was supposedly sent from there.

Wikileaks 2008

Had domain name shut down by a federal judge for leaking documents detailing tax evasion in the Cayman Islands by major US political celebrities. Injunction lifted after much protest

New York Times Aug 8, 2008

“WASHINGTON – The Federal Bureau of Investigation said Friday that it has improperly obtained the phone records of reporters for the New York Times and Washington Post in the Newspapers' Indonesia Bureaus in 2004.”

An initial report by the inspector general found that the FBI had violated its own policies in tens of thousands of cases

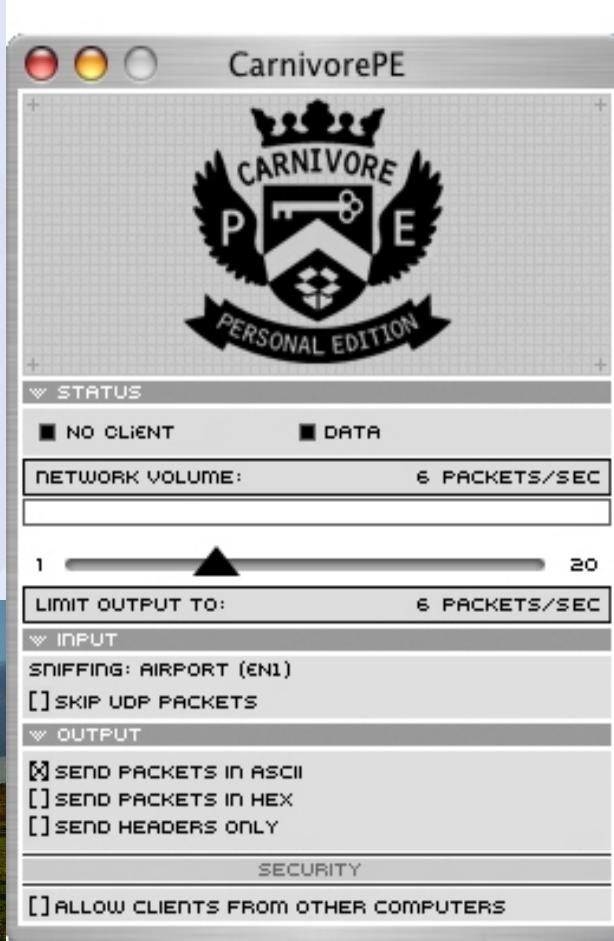
Josh Wolf 2006

Wolf served 226 days in prison at the Dublin FCI (California) for refusing to divulge source material. This made him the longest-imprisoned journalists for refusing to do so in US history.

FBI Raids Indymedia

On October 7, 2004 the FBI seized the servers used by a number of IMCs and hosted by US-based Rackspace Managed Hosting. Indymedia was not notified prior to the raid and over 50 websites were taken offline as a result.

Echelon, Carnivore



```
:CarnivorePE:15:44:21 213.165.65.100.80 >
192.168.178.23.49868 == YX'A
:CarnivorePE:15:44:21 213.165.65.211.80 >
192.168.178.23.49870 ==
:CarnivorePE:15:44:21 213.165.65.211.80 >
192.168.178.23.49870 == HTTP/1.0 302
Moved Content-Location: http://
images.gmx.net/images/bs/23842/topscout-homes.gif Location: http://images.gmx.net/images/bs/23842/topscout-homes.gif Server: GMX Banner V1.9 Connection: close Date: Sun, 25 Sep 2005 13:42:18 GMT Last-Modified: Sun, 25 Sep 2005 13:42:17 GMT
:CarnivorePE:15:44:21 192.168.178.23.49870 >
213.165.65.211.80 ==
:CarnivorePE:15:44:21 213.165.65.211.80 >
192.168.178.23.49870 ==
:CarnivorePE:15:44:21 192.168.178.23.49870 >
213.165.65.211.80 ==
:CarnivorePE:15:44:21 213.165.65.211.80 >
192.168.178.23.49869 ==
:CarnivorePE:15:44:21 213.165.65.211.80 >
192.168.178.23.49870 == $
:CarnivorePE:15:44:22 213.165.65.100.80 >
192.168.178.23.49851 ==
:CarnivorePE:15:44:22 213.165.65.100.80 >
192.168.178.23.49850 ==
```

Nothing to see here

Identity

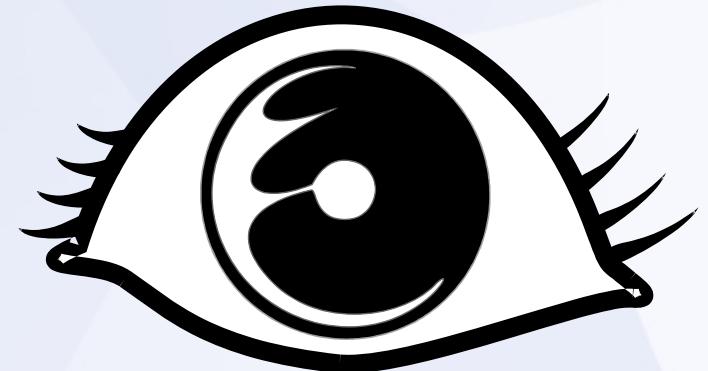
- *What you are known as*
- *Complex*
- *Often un-authenticated*
- *Anonymity v pseudonymity*



we all have one

Keeping an Eye on Your Data

- *Who wants access to your information? Why?*
- *Who do you want to have access? Why?*
- *Think about cops, private investigators, marketers, creeps, and others*



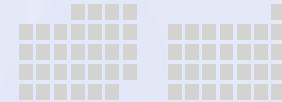
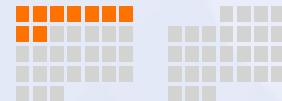
Nothing to see here

Firefox

- *Free software*
- *Cool plugins*
- *Cross-platform*

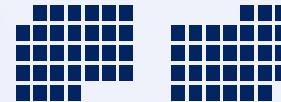


Firefox



9
days of risk

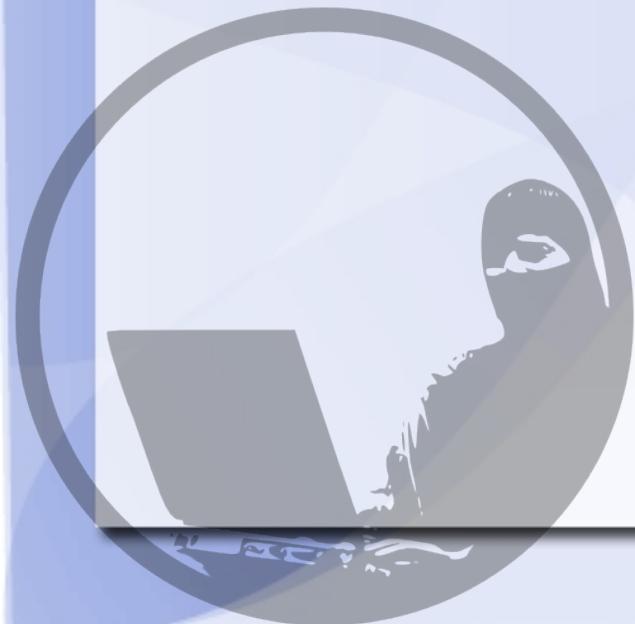
Internet Explorer



284
days of risk

Anti-Malware Software

- *How it works*
- *Who needs it?*
- *AVG Free Edition*
- *Malwarebytes Anti-Malware*
- *Not worth paying for*



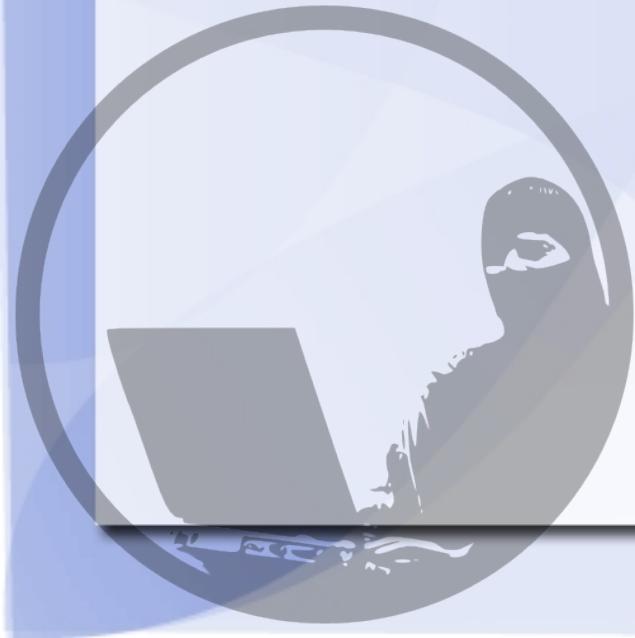
Secure File Deletion

- *Delete vs Wipe*
- *Eraser, srm/wipe, OS X ctrl-click*
- *Will not clear swap, logs, filesystem data, temp files, etc*
- *DBAN for entire drive*
- *Recovering after wiping?*
- *Avoid wiping by encrypting first!*



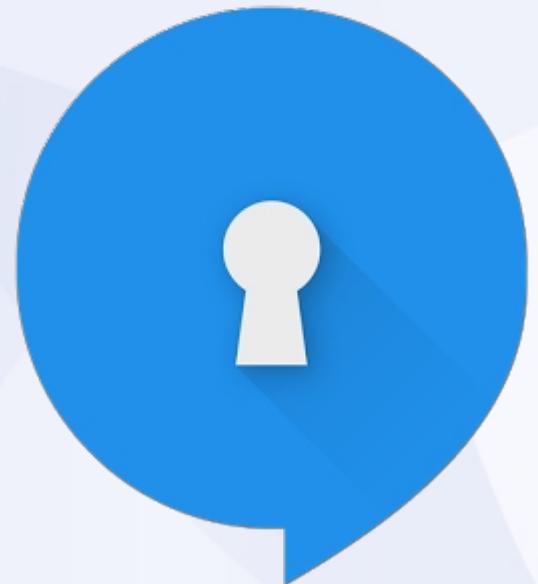
General Warning on Phones

- *Security Patches*
- *Backdoors and closed-source*
- *Monitoring by telcos, location info*
- *Some security > none*



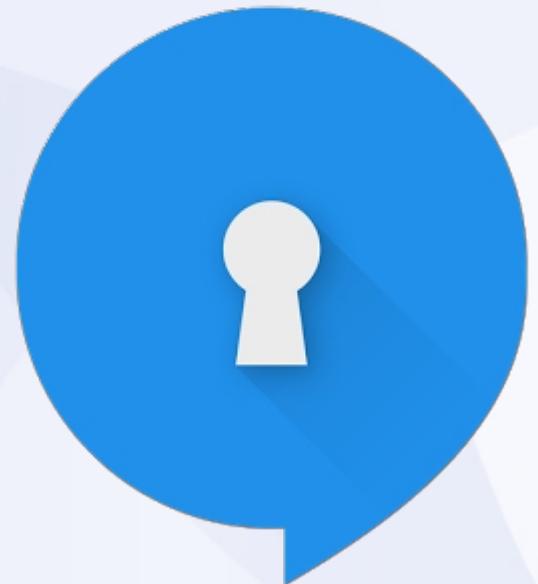
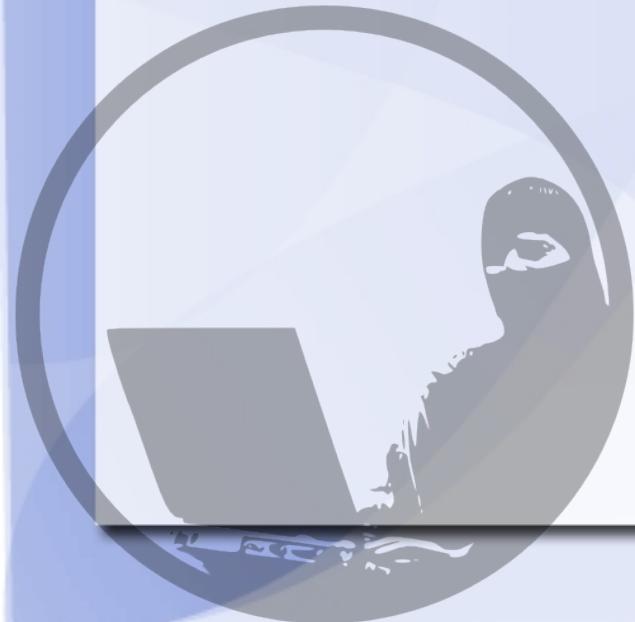
What is Signal?

- *Developed by Whisper Systems*
- *Encrypts texts in transit*
- *Supports media texts*
- *Saves you if on limited text plan*
- *Android + iOS*
- *Encrypted phone calls*



What does it not protect against?

- *Somebody knowing who you're talking to*
 - *People without signal*
 - *Phone seizure*



What is Tor?

- *Originally developed by the Navy*
- *High degree of anonymity*
- *For web and other traffic*
- *Allows hosting of hidden services*



Tor's Protections

- *Protects you from people knowing who you communicate with or what you say to them*
- *Provides online anonymity*
- *Protects you from filtering*



Tor's Weaknesses

- *Physical seizure*
- *Misplaced trust in hardware/software*
- *Global adversary/node timing*
- *Insecure physical surroundings*
- *User error/writing analysis*
- *External files*





How Tor Works: 3



Alice



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.

Again, **green links** are encrypted, **red links** are in the clear.

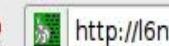
Dave



Jane



Bob



Most Visited ▾ Getting Started

| Forums Tor Links Preferences Your Messages Members Today's Topics New Posts Search Calendar | | | | | |
|--|---|--------|---------|--|--|
| Guest, do not forget to login (Register) | | | | | |
| Administration | | | | | |
| | Forum | Topics | Replies | Last Post Info | |
| | How To Post!! | 0 | | | |
| | Announcements anything and every administrative | 26 | 40 | » Aug 17, 2008, 9:39 am in: ideas by: Guest | |
| | Policies Ste Policies | 1 | 7 | » Aug 9, 2008, 10:26 am in: Policy overview by: Guest | |
| The onionforum | | | | | |
| | Forum | Topics | Replies | Last Post Info | |
| | TOR Anything and everything about tor | 294 | 1424 | » Aug 17, 2008, 1:54 pm in: Onion Weed by: theoutsider | |
| | News Talk about the news and current events | 94 | 111 | » Aug 13, 2008, 1:41 am in: Incognito CD by: Guest | |
| | Sports and Games computer games, board games, and sports games | 5 | 19 | » Jul 24, 2008, 7:29 pm in: The death of content by: Guest | |
| | Politics | 21 | 97 | » Aug 13, 2008, 1:43 am in: Gun for hire | |

[Home](#)[About Tor](#)[Documentation](#)[Projects](#)[Press](#)[Blog](#)[Store](#)[Download](#)[Volunteer](#)[Donate](#)

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

[Download Tor](#)

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as [traffic analysis](#).

[Learn more about Tor ...](#)

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning

Who Uses Tor?



Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.



Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal accountability.



Activists

Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report on corruption.



Media

Journalists and the media use Tor to

[Home](#) [About Tor](#) [Documentation](#) [Projects](#) [Press](#) [Blog](#) [Store](#)[Download](#) [Volunteer](#) [Donate](#)

HOME » DOWNLOAD

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the [full list of warnings](#) for details.

Tor Browser Bundle for Windows

Version 2.2.35-12 - Windows 7, Vista, and XP

Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run. [Learn more »](#)

Not Using Windows? Download for [Mac](#) or [Linux](#)



BROWSER
BUNDLE

Download

Tor Browser Bundle

 What's This? English 

Looking For Something Else? [View All Downloads](#)

Donate to Tor

\$

One-time Donation 

Donate

[Other donation options...](#)

► Microsoft Windows

► Apple OS X

► Linux/Unix

► All Downloads



Download Tor



torproject.org

https://www.torproject.org/download/download-easy.html.en



Google



Home

About Tor

Documentation

Projects

Press

Blog

Store

Download

Volunteer

Donate

HOME » DOWNLOAD

Want Tor to re

You need to change
warnings for details

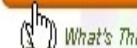
Tor Brow

Version 2.

Everything you need to safely browse the Internet. This package
requires no installation. Just extract it and run. [Learn more »](#)Not Using Windows? Download for [Mac](#) or [Linux](#)

Download

Tor Browser Bundle



What's This?

English

Looking For Something Else? [View All Downloads](#)

Donate to Tor

5

the Donation

Donate

More donation options...

▶ Microsoft Windows

▶ Apple OS X

▶ Linux/Unix

▶ All Downloads



Download Tor



Home About Tor Documentation Projects Press Blog Store

[Download](#)[Volunteer](#)[Donate](#)**Open Executable File?**

"tor-browser-2.2.35-12_en-US.exe" is an executable file. Executable files may contain viruses or other malicious code that could harm your computer. Use caution when opening this file. Are you sure you want to launch "tor-browser-2.2.35-12_en-US.exe"?

 Don't ask me this again[OK](#)[Cancel](#)

HOME » DOWNLOAD

Want Tor

 You need to warnings to

0 Tor

\$ 5

One-time Donation

[Donate](#)[Other donation options...](#)**Tor Browser Bu**

Version 2.2.35-12 - V

Everything you need to safely browse the web. It's fast, private, and requires no installation. Just extract and go.

Not Using Windows? D

Lookin

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?



Name: tor-browser-2.2.35-12_en-US.exe

Publisher: **Unknown Publisher**

Type: Application

From: C:\Documents and Settings\user\My Documents\Down...

[Run](#)[Cancel](#) Always ask before opening this file

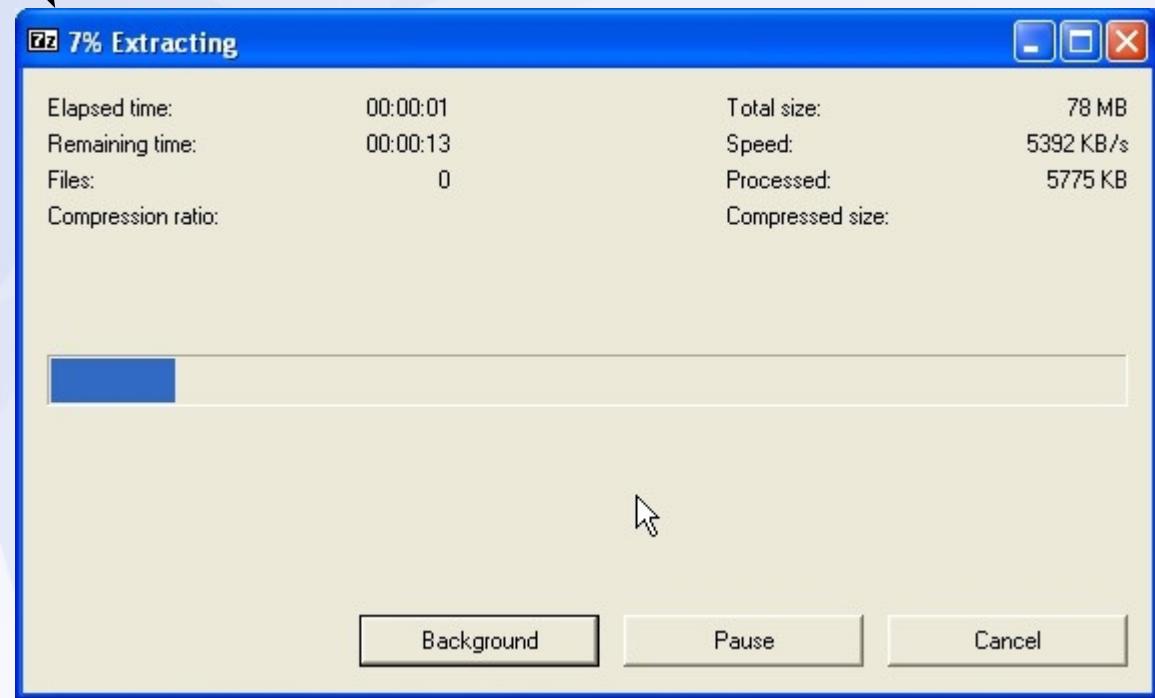
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. [How can I decide what software to run?](#)

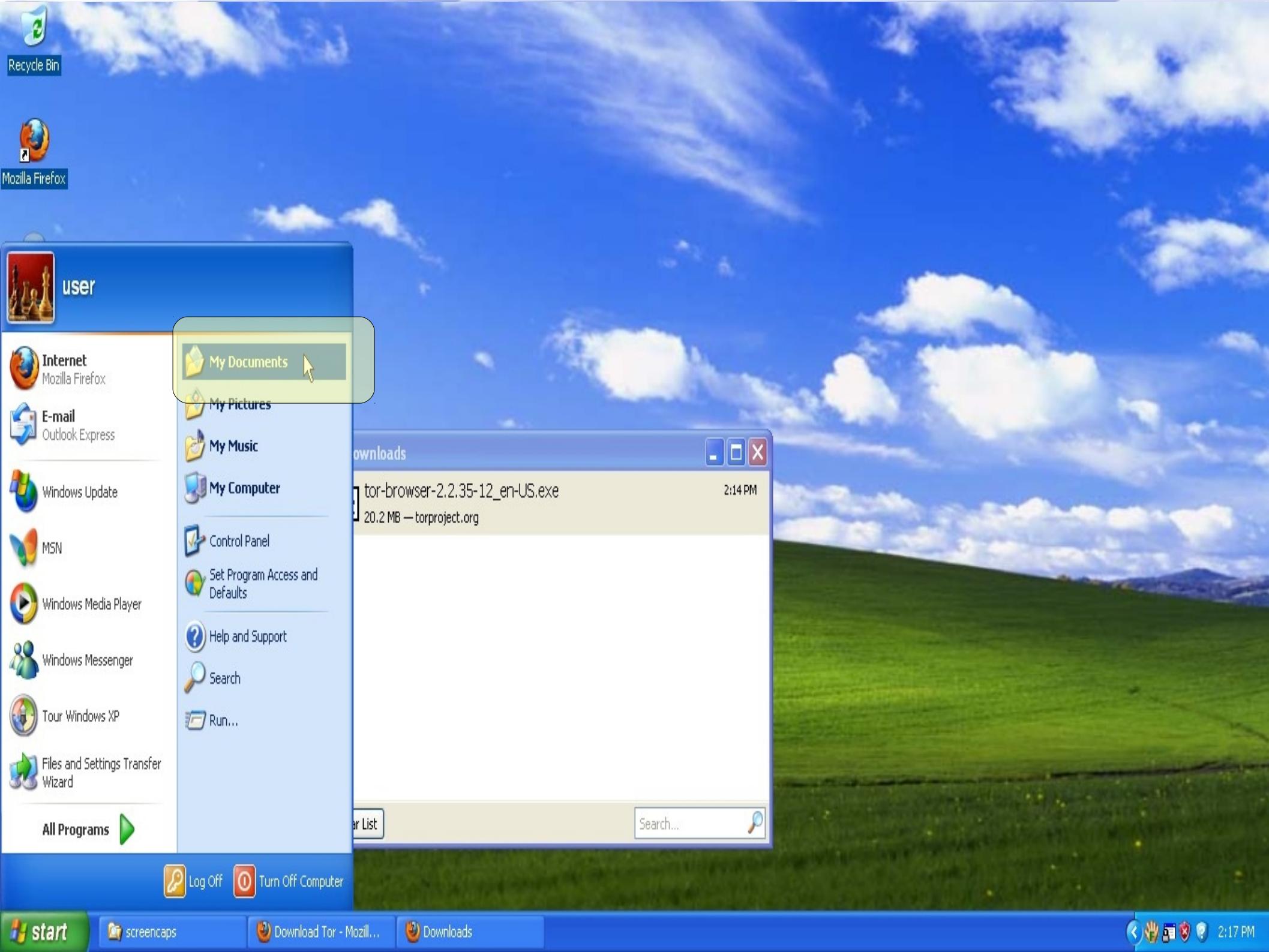
Microsoft Windows

Apple OS X

Linux/Unix

All Downloads





Recycle Bin



Mozilla Firefox



user



Internet
Mozilla Firefox



E-mail
Outlook Express



Windows Update



MSN



Windows Media Player



Windows Messenger



Tour Windows XP



Files and Settings Transfer Wizard



All Programs



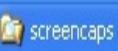
Log Off



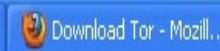
Turn Off Computer



start



screencaps



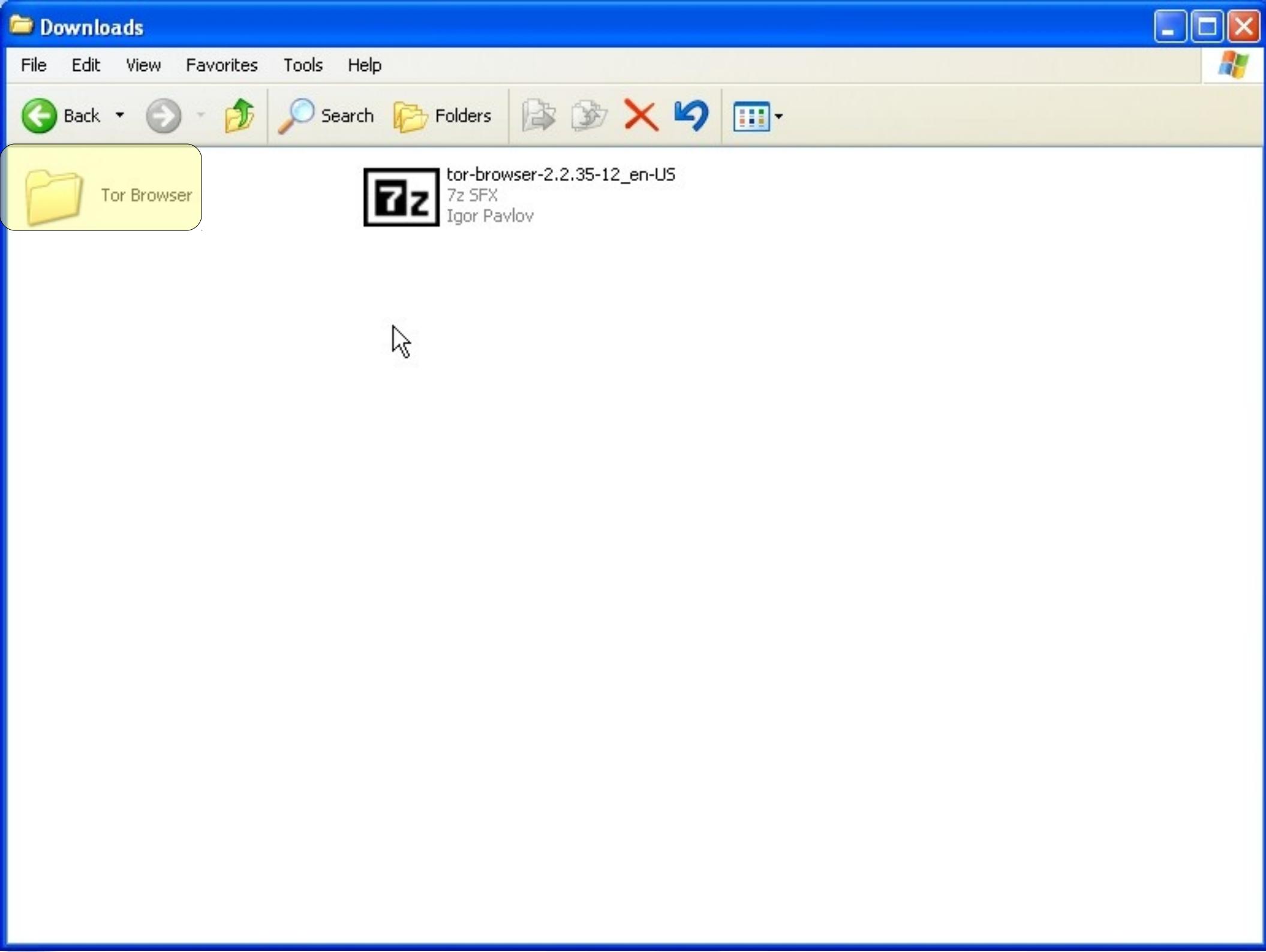
Download Tor - Mozilla...



Downloads

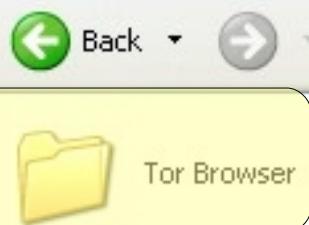


2:17 PM



Downloads

File Edit View Favorites Tools Help



 tor-browser-2.2.35-12_en-US
7z SFX
Igor Pavlov

Download Tor

torproject.org https://www.torproject.org/download/download-easy.html.en

Home

HOME » DOWNLOAD

Want Tor to really work?

You need to change some of your habits, as some things won't work. [warnings](#) for details.

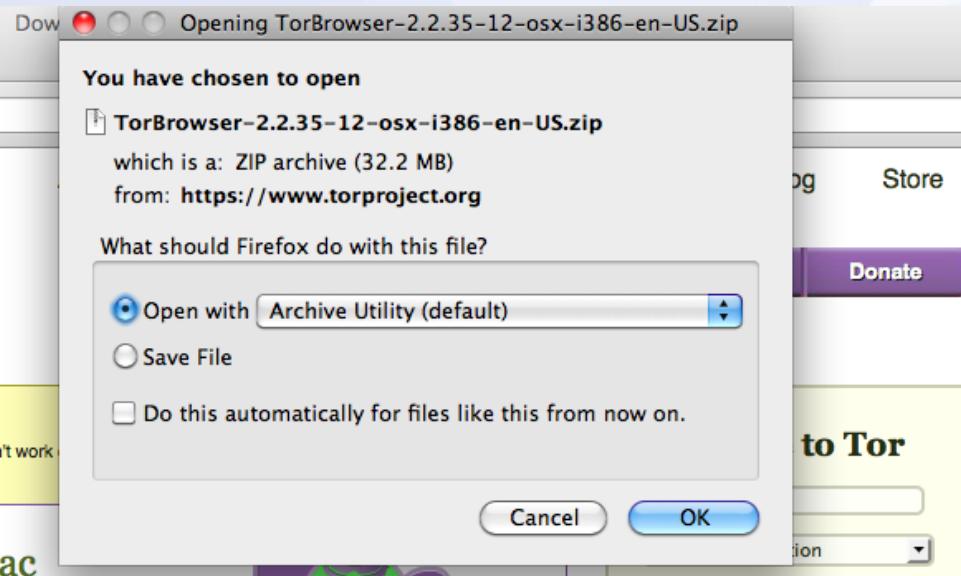
Tor Browser Bundle for Mac
Version 2.2.35-12 - OS X

Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run. [Learn more »](#)

Not Using Mac? Download for [Windows](#) or [Linux](#)

Tor Browser Bundle for 64-Bit Mac
Version 2.2.35-12 - OS X (64-Bit)

Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run. [Learn more »](#)



to Tor

Donate [Other donation options...](#)

▶ Microsoft Windows
▶ Apple OS X
▶ Linux/Unix
▶ All Downloads

Having Trouble?

▶ Read the fine manuals

Download Tor

[torproject.org](https://www.torproject.org) https://www.torproject.org/download/download-easy.html.en

star C tor pro



HOME » DOWNLOAD

You need to change s
warnings for details.

Tor Brow

Everything you need
package requires no in
[more »](#)

Not Using Mac'



TorBrowser_en-US

2

Downloads



2 items, 82.54 GB available

Apple OS X

▶ Linux/Unix

▶ All Downloads

Tor Browser Bundle for 64-Bit Mac

Version 2.2.35-12 - OS X (64-Bit)

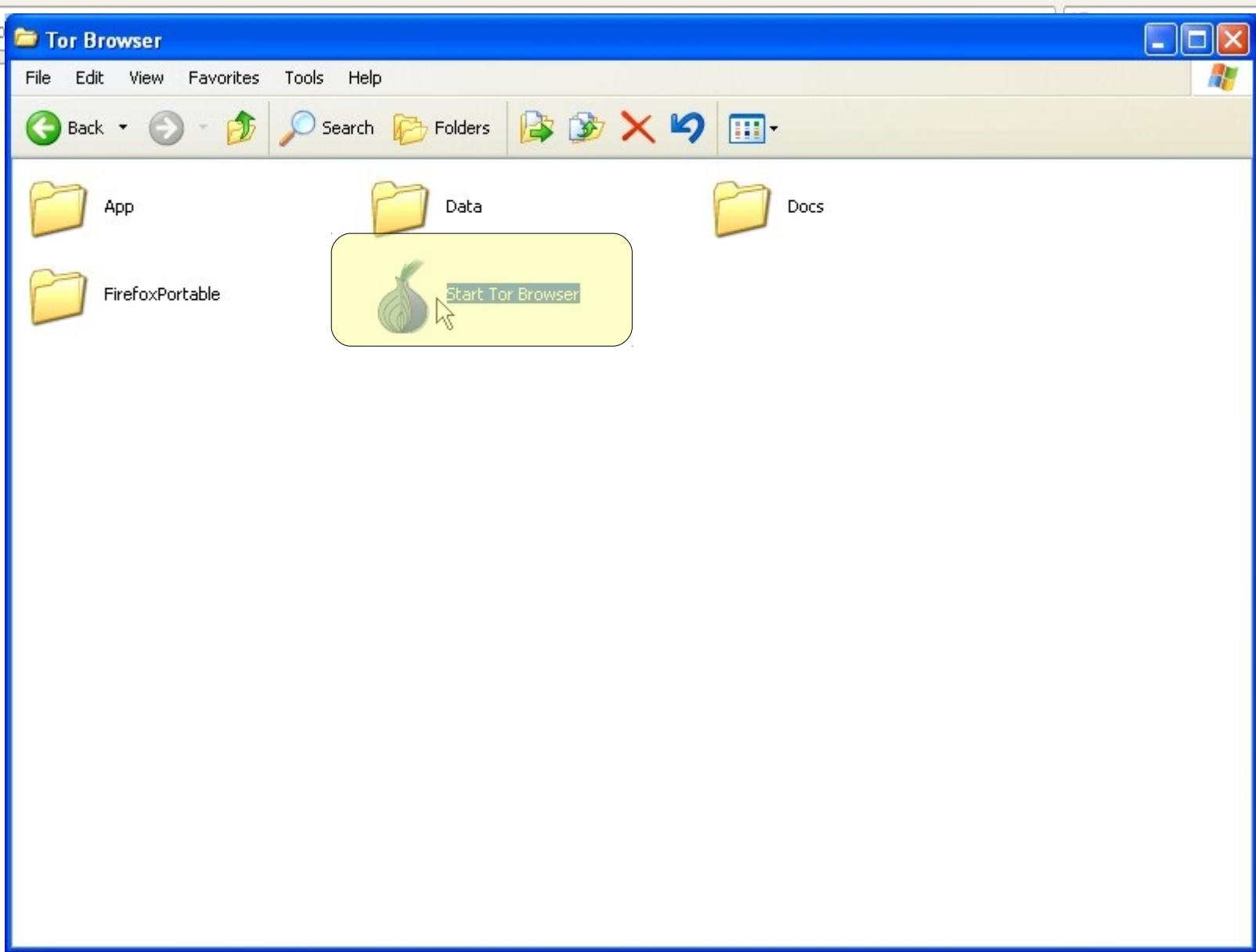
Everything you need to safely browse the Internet. This
package requires no installation. Just extract it and run. [Learn
more »](#)



Download
Mac 64-bit

Having Trouble?

▶ Read the fine manuals



privacy, confidential business activities and relationships, and state security known as traffic analysis

[Learn more about Tax](#)

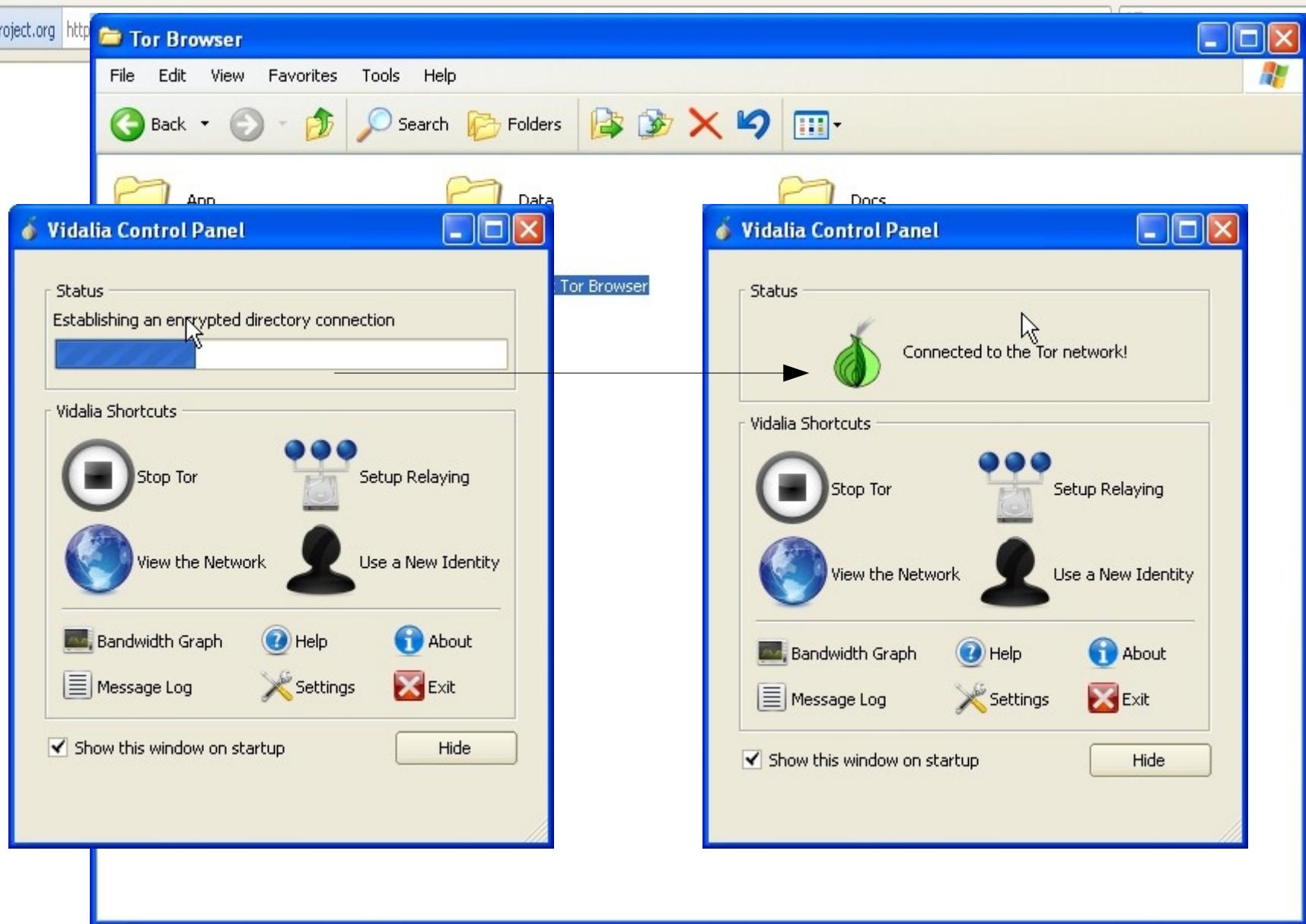
prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of

report on corruption.



Media

Journalists and the media use Tor to



privacy, confidential business activities and relationships, and state security known as traffic analysis

[Learn more about Tax](#)

prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of

report on corruption.



Media

Journalists and the media use Tor to

Are you using Tor?

Startpage



Congratulations. Your browser is configured to use Tor.



Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously.

Your IP address appears to be: 77.247.181.162

This page is also available in the following languages:

[العربية \(Arabiya\)](#) [Burmese](#) [češky](#) [dansk](#) [Deutsch](#) [Ελληνικά \(Ellinika\)](#) [English](#) [español](#) [Estonian](#) [فارسی \(Farsi\)](#) [suomi](#) [français](#) [Italiano](#) [日本語 \(Nihongo\)](#) [norsk \(bokmål\)](#) [Nederlands](#) [polski](#) [Português](#) [Português do Brasil](#) [română](#)
[Русский \(Russkij\)](#) [Thai](#) [Türkçe](#) [Українська \(ukrajins'ka\)](#) [Vietnamese](#) [中文\(简\)](#)



IP CHICKEN

Served fresh daily.TM[CURRENT IP](#) | [SECURITY PORT SCAN](#) | [HELP](#)

Current IP Address

77.247.181.162[Add to Favorites](#)

Advanced

- Name Address: chomsky.torservers.net
- Remote Port: 46001
- Browser: Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0

Encrypting Online Chat

- We will use *Pidgin* + Off-The-Record
- Similar weaknesses to Tor
- Private key compromise only compromises most recent conversation
- Only works for 1-on-1 conversations

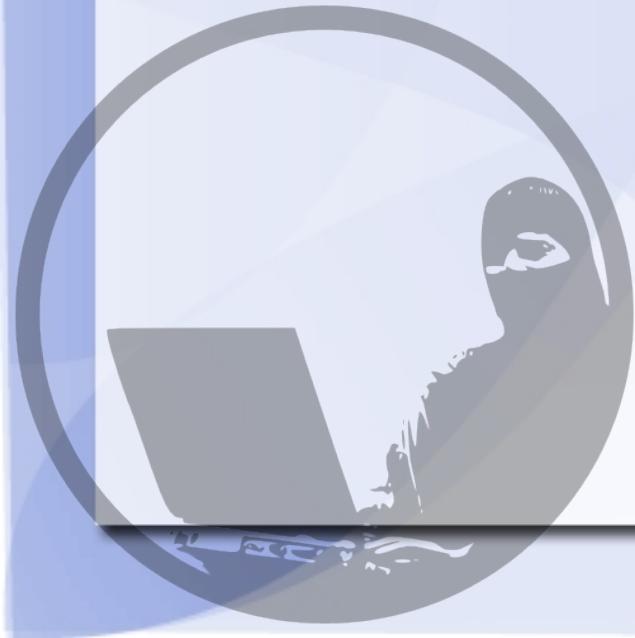


q
i
d
g
i
n



Pidgin+OTR Protections

- *Protects you from people knowing what you're saying*
- *Protects you by authenticating who you're talking to*
- *Does not protect you from people knowing who you are talking to*



q
i
d
q
i
n

File Edit View History Bookmarks Tools Help

Pidgin, the universal chat client



pidgin.im



Google



DOWNLOAD

PLUGINS

HELP

ABOUT

NEWS

DEVELOPMENT



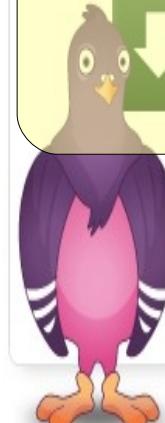
pidgin
2.10.4

 Download Now

sourceforge - Trusted for Open Source

2.10.4 for Windows

[ChangeLog](#)



IM all your friends in one place

Pidgin is an easy to use and free chat client used by millions. Connect to AIM, MSN, Yahoo, and more chat networks all at once.

Supported chat networks:

- AIM
- Google Talk
- IRC
- MySpaceIM
- Sametime
- Zephyr
- Bonjour
- Groupwise
- MSN
- SILC
- XMPP
- Gadu-Gadu
- ICQ
- Mixit
- SIMPLE
- Yahoo!

Learn More ➔

Pidgin 2.10.4 contains [two security](#)

File Edit View History Bookmarks Tools Help

Download Pidgin from SourceForge.net



sourceforge.net/projects/pidgin/files/Pidgin/2.10.4/pidgin-2.10.4.exe/download?accel_key=62%3A1337894520%3Ahttp%253A//pidgin.im/%3A7e819905%24a7b564ffbc9d6bf6b42cf4f

Google



SOURCEFORGE

Find Open Source Software

Browse Blog Support Jobs Newsletters Resources

Register Log In



Your Pidgin download will start shortly...

Opening pidgin-2.10.4.exe

You have chosen to open

pidgin-2.10.4.exe

which is a: Binary File (8.9 MB)
from: http://voxel.dl.sourceforge.net

Would you like to save this file?

Save File

Cancel

41% of 1 file - Downloads

pidgin-2.10.4.exe

14 seconds remaining — 3.7 of 8.9 MB (365 KB/sec)

Clear List

Search...

Downloads

pidgin-2.10.4.exe
8.9 MB — sourceforge.net

2:22 PM

Download Manager



Off-the-Record Messaging

News Downloads Mailing Lists Documentation FAQ Press Software People

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

① Encryption

No one else can read your instant messages.

② Authentication

You are assured the correspondent is who you think it is.

③ Deniability

The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.

④ Perfect forward secrecy

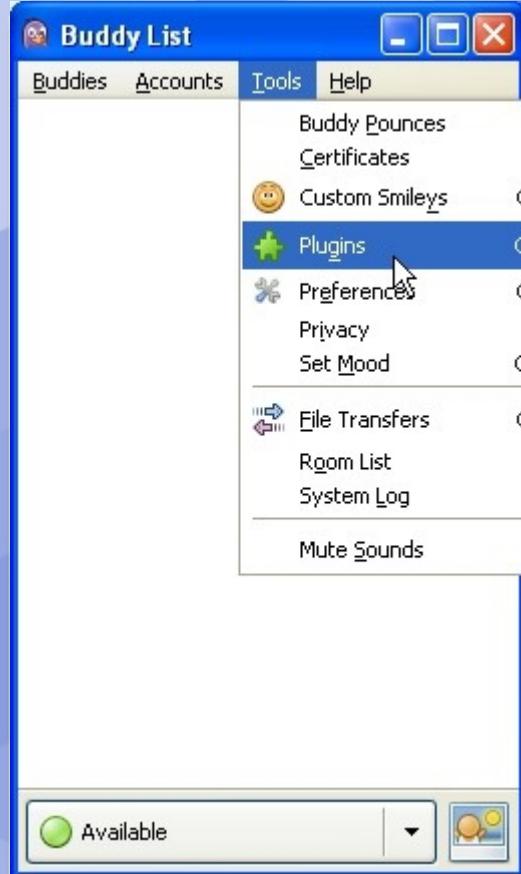
If you lose control of your private keys, no previous conversation is compromised.

Primary download: Win32 installer for pidgin-otr 3.2.1 [other downloads]

News

16 May 2012 Security update: pidgin-otr version 3.2.1

<http://www.cypherpunks.ca/otr/binaries/windows/pidgin-otr-3.2.1-1.exe> in-otr plugin contain a format string security flaw. This flaw could potentially be exploited by a remote attacker to cause arbitrary code to be



Plugins

| Enabled | Name | Description |
|-------------------------------------|---|---|
| <input type="checkbox"/> | Message timestamp formats 2.10.4 | Customizes the message timestamp formats. |
| <input type="checkbox"/> | New Line 2.10.4 | Prepends a newline to displayed message. |
| <input checked="" type="checkbox"/> | Off-the-Record Messaging 3.2.1 | Provides private and secure conversations |

Off-the-Record Messaging
Enhances the privacy of IM communications by providing encryption, authentication, deniability, and security.
Developed by Rob Smits, Chris Alexander, Nikita Borisov
cotr@cypherpunks.ca>

Plugin Details

- Psychic Mode** 2.10.4
Psychic mode for incoming conversation
- Release Notification** 2.10.4
Checks periodically for new releases.
- Send Button** 2.10.4
Conversation Window Send Button.
- Text replacement** 2.10.4
Replaces text in outgoing messages according to user-defined rules.
- Timestamp** 2.10.4
Display iChat-style timestamps
- Transparency** 2.10.4
Variable Transparency for the buddy list and conversations.
- Windows Pidgin Options** 2.10.4
Options specific to Pidgin for Windows.
- XMPP Console** 2.10.4

Configure Plugin **Close**

Buddy List

Buddies Accounts Tools Help

- New Instant Message... Ctrl+M
- Join a Chat... Ctrl+C**
- Get User Info... Ctrl+I
- View User Log... Ctrl+L
- Show ▾
- Sort Buddies ▾
- Add Buddy... Ctrl+B
- Add Chat...
- Add Group...
- Quit Ctrl+Q

Join a Chat

Please enter the appropriate information about the chat you would like to join.

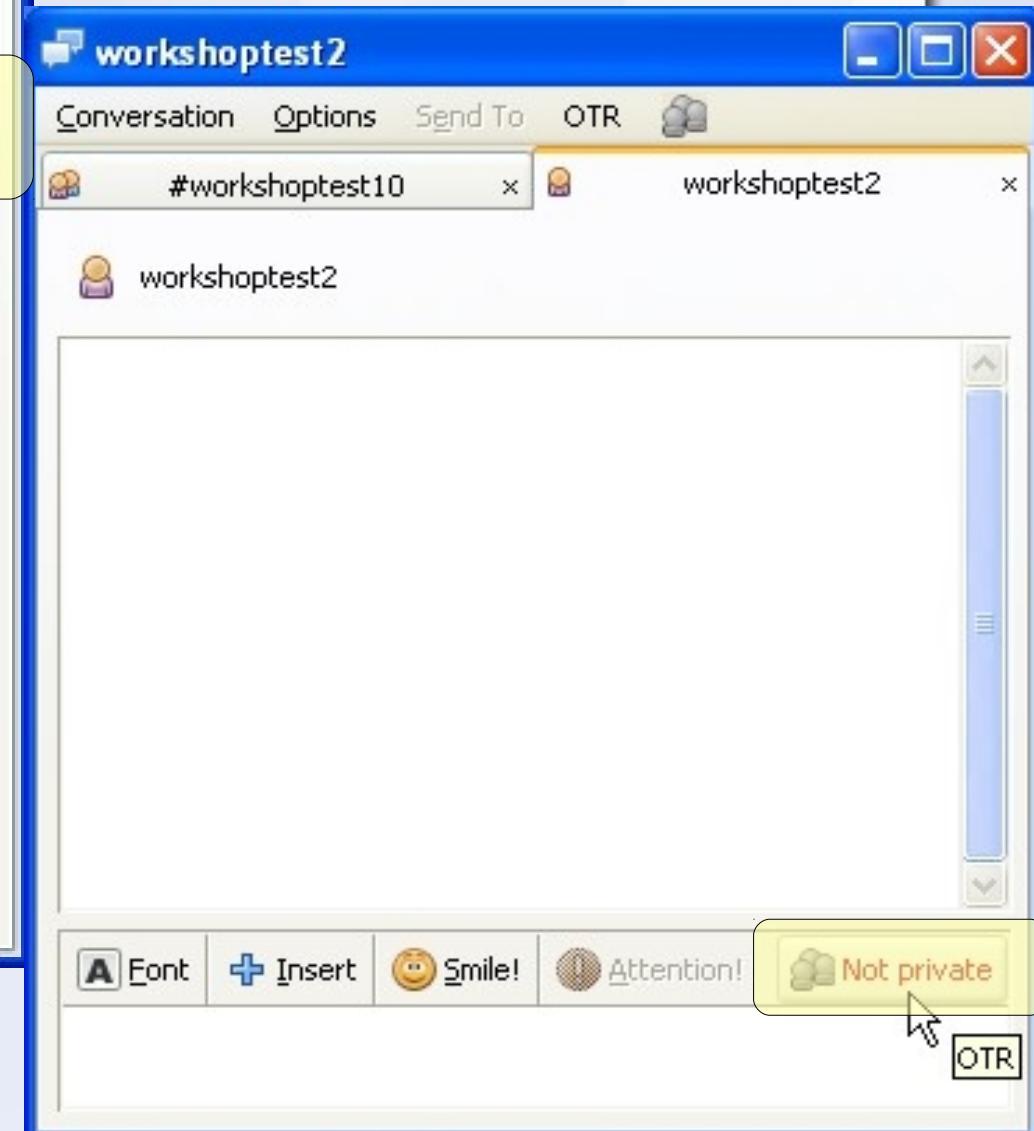
 Account:

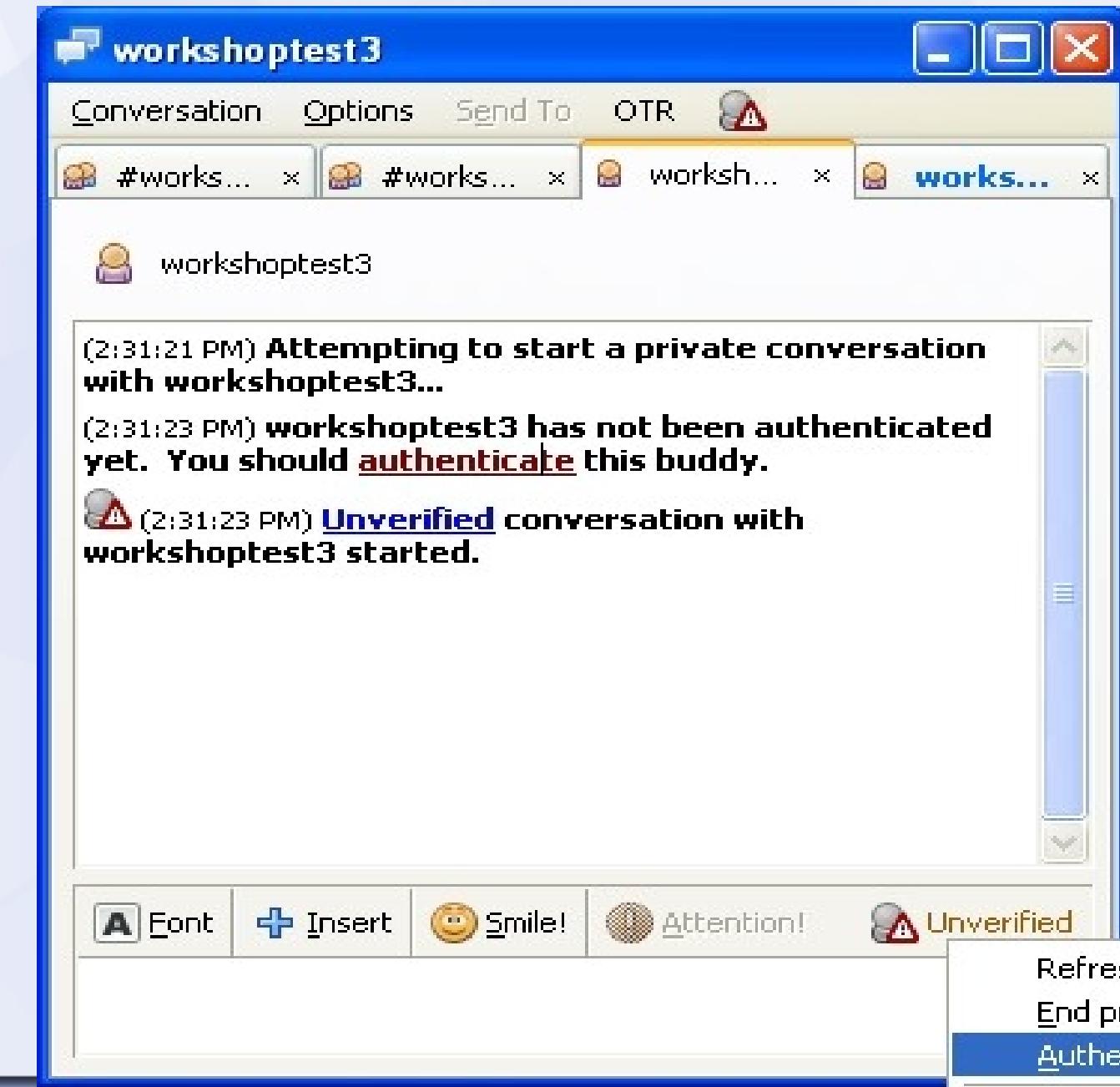
Channel:

Password:

Room List Cancel Join

Available





 Authenticate Buddy

Authenticate workshoptest3

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?

Question and answer

To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.

Enter question here:

What is your gmail address?

Enter secret answer here (case sensitive):

supersecretemail@gmail.com

[Help](#) [Cancel](#) [Authenticate](#)

 Authenticate Buddy

Authentication from workshoptest2

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

Your buddy is attempting to determine if he or she is really talking to you, or if it's someone pretending to be you. Your buddy has asked a question, indicated below. To authenticate to your buddy, enter the answer and click OK.

This is the question asked by your buddy:
What is your gmail address?

Enter secret answer here (case sensitive):

supersecretemail@gmail.com

[Help](#) [Cancel](#) [Authenticate](#)



workshoptest3



Conversation Options Send To OTR



#works...



#works...



worksh...



worksh...



workshoptest3

(2:31:21 PM) **Attempting to start a private conversation with workshoptest3...**

(2:31:23 PM) **workshoptest3 has not been authenticated yet. You should authenticate this buddy.**

(2:31:23 PM) **Unverified conversation with workshoptest3 started.**

(2:33:39 PM) **The privacy status of the current conversation is now: Private**



Font



Insert



Smile!



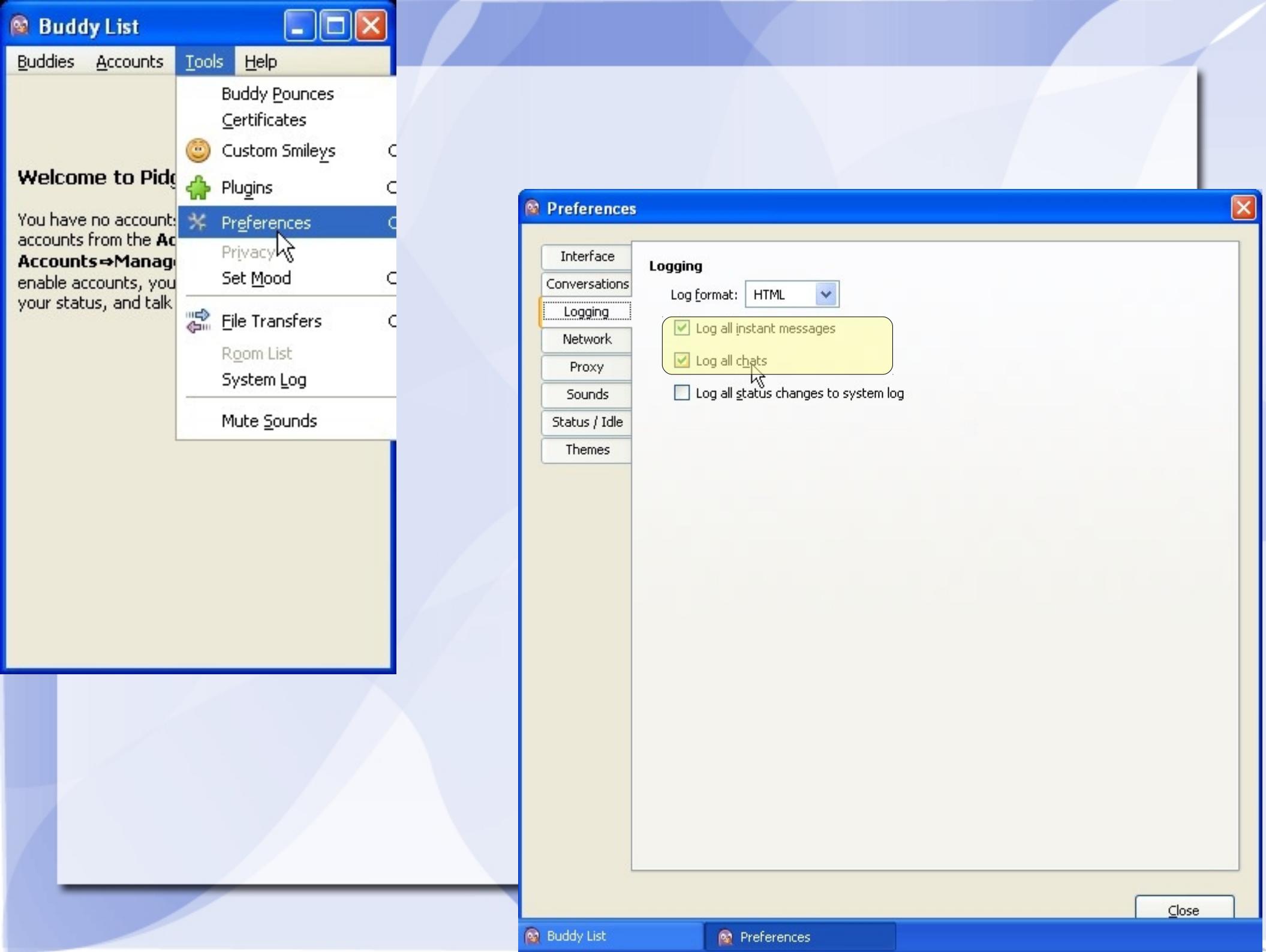
Attention!



Private

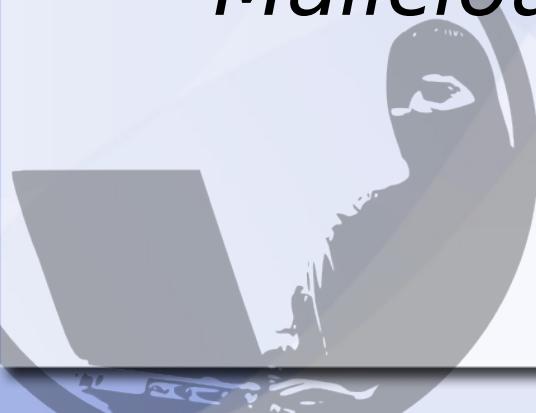


OTR



Introducing...Cryptocat

- *Protects you from people knowing what you're saying or who you're talking to (but not who you are)*
- *Cross-platform*
- *No installation/configuration required*
- *Available as a Tor hidden service*
- *Malicious server weakness*

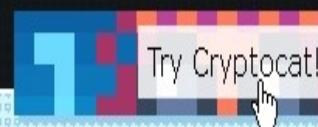




Chat with privacy.

Converse with your friends, partners and co-workers in privately and securely, in an instant messaging environment that offers encryption without sacrificing accessibility.

Cryptocat is a new, free, open experiment that aims to let you do just that.
Watch the video!

[Home](#)[About Cryptocat](#)[Documents](#)[Blog](#)[Source Code](#)

Cryptocat

Access from any desktop or mobile browser, or set up your own server.

Cryptocat for Chrome Best Option

Integrates with Google Chrome for faster, safer instant messaging.

Cryptocat for Android Under Development

Use your Android device for quick, secure access to encrypted chat.

What is Cryptocat?

Cryptocat is free software that aims to provide an open, accessible Instant Messaging environment with a transparent layer of encryption that works right in your browser.

Aw fiddlesticks!

This video can't be played with your current setup.

Please switch to a browser that provides native H.264 support.

Who Uses Cryptocat?



Friends & Family

Cryptocat means to be as accessible as any other web Instant Messaging platform, while also offering a transparent layer of security. This makes it an ideal alternative to invasive services for talking with friends and family.



Nonprofits

Nonprofit organizations regularly require private communications, but often deal with parties that



CRYPTOCAT

supersecretplace

enter

?

New to Cryptocat? Check out this [cool video!](#)



Cryptocat lets you instantly set up secure conversations. It's an open source encrypted, private alternative to other services such as Facebook chat.



Messages are encrypted inside your own browser using AES-256. Encrypted data is securely wiped after one hour of inactivity.



Cryptocat also runs as a [Tor hidden service](#) (<http://xdtfje3c46d2dnjd.onion>) and works on your iPhone, Android and BlackBerry.

File Edit View History Bookmarks Tools Help

[-] Cryptocat



▼

G



crypto.cat https://crypto.cat/?c=supersecretplace

CRYPTOCAT



Enter nickname

captainspy I chat

chatting as captainspy on https://crypto.cat/?c=supersecretplace

256



CRYPTOCAT



Type on your keyboard as randomly as possible for a few seconds:

chatting as captainspy on https://crypto.cat/?c=supersecretplace

256



CRYPTOCAT

For more information on how Cryptocat works and its limitations, please visit the [project website](#).

> captainspy has arrived

captainspy lalalala I'm chatting to myself and this time... nobody has to know
BWAHAHAHAHAHA!

chatting as captainspy on https://crypto.cat/?c=supersecretplace

1 captainspy

256

The screenshot shows a web browser window displaying the Cryptocat application. The title bar reads "[-] Cryptocat - Mozilla Firefox". The main content area is a black-bordered window titled "CRYPTOCAT". Inside, there's a message from "captainspy" stating "captainspy has arrived". Below it, another message from "captainspy" says "lalalala I'm chatting to myself and this time... nobody has to know BWAHAHAHAHAHA!". At the bottom, the status bar shows "chatting as captainspy on https://crypto.cat/?c=supersecretplace". A message input field contains "@captainspy I'm sending you a private message!" and a counter indicates "211" messages sent.

CRYPTOCAT

For more information on how Cryptocat works and its limitations, please visit the project website.

> captainspy has arrived

captainspy lalalala I'm chatting to myself and this time... nobody has to know
BWAHAHAHAHAHA!

chatting as captainspy on https://crypto.cat/?c=supersecretplace

1 captainspy

@captainspy I'm sending you a private message! T

211

 CRYPTOCAT

For more information on how Cryptocat works and its limitations, please visit the project website.

> captainspy has arrived

captainspy lalalala I'm chatting to myself and this time... nobody has to know
BWAHAHAHAHAHA!

captainspy > captainspy I'm sending you a private message

chatting as captainspy on https://crypto.cat/?c=supersecretplace

1 captainspy

I

256

What is Encryption Anyways?

- *A way of encoding information*
- *Makes eavesdropping much more difficult*
- *Generally prevents your adversary from knowing what you're saying but not who you're saying it to.*



Nothing to see here

Examples of Encryption

- *Code Words*
- *Caesar Cipher (Shared key)*
- *WWII Enigma Machines*
- *HTTPS/SSL (Public Key)*
- *PGP (Public Key)*

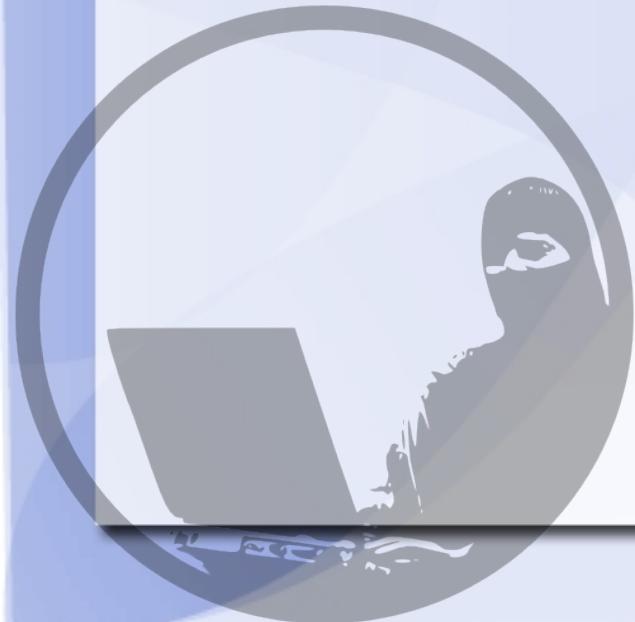


Nothing to see here

Caesar Cipher

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | A |
| T | H | I | S | I | S | A | S | E | C | R | E | T | M | E | S | S | A | G | E | | | | |
| U | I | J | T | J | T | B | T | F | D | S | F | U | N | F | T | T | B | H | F | | | | |

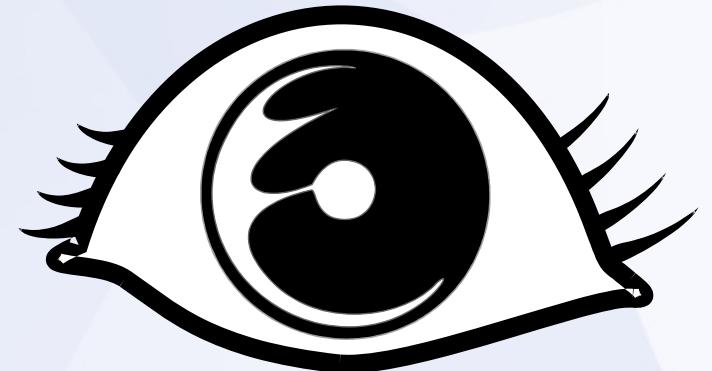
Example: Shift up to encrypt
Shift down to decrypt
Shared secret system



Nothing to see here

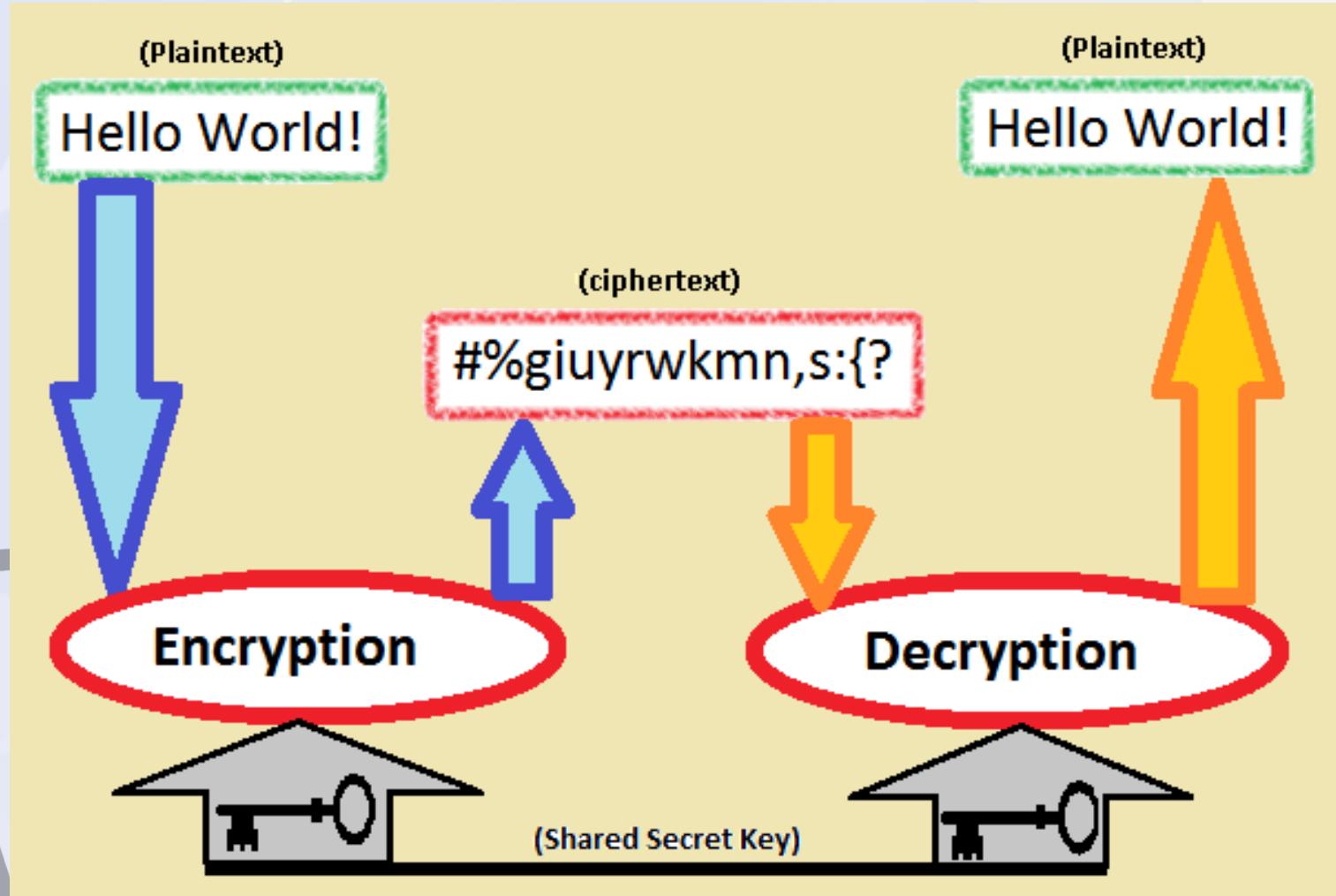
What Does it Protect Me From?

- *Seizure of information*
- *Interception of communications*
- *Un-authenticated communications*
- *Is not foolproof and is always better to not store the information in the first place!*



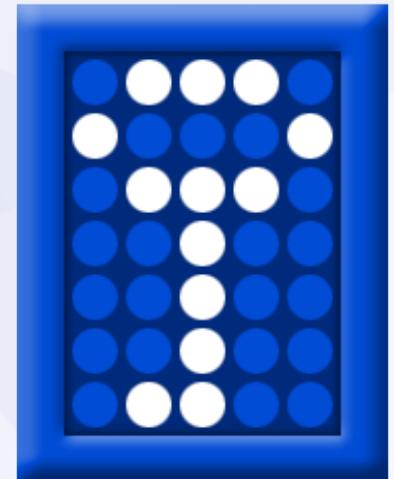
Nothing to see here

So what does it look like?



TrueCrypt & VeraCrypt

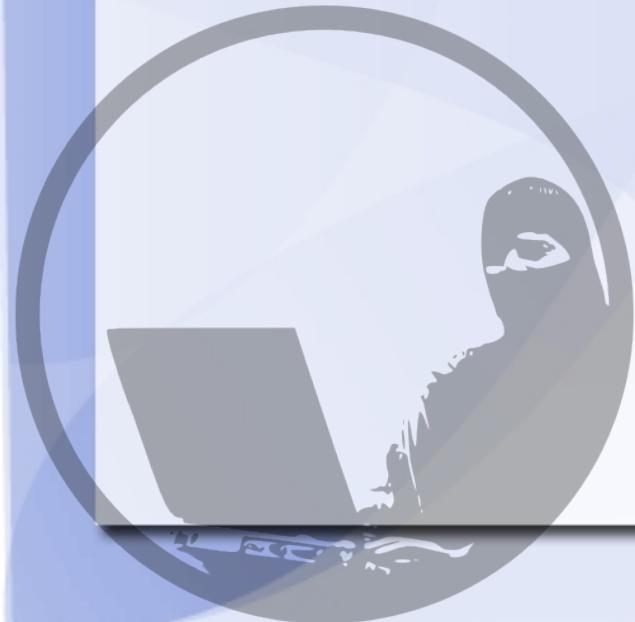
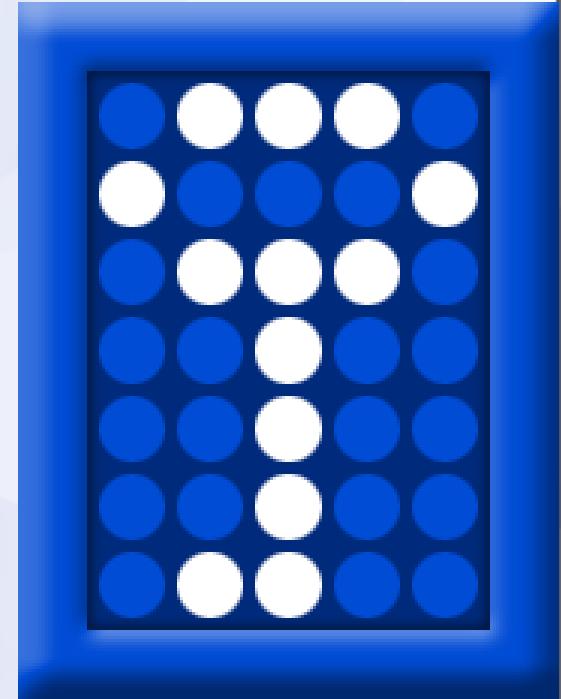
- *Makes encrypted “volumes” from files and drives.*
- *Transparent & plausibly deniable*
- *Open source & cross-platform*
- *Offers full disk encryption (Windows), “hidden volumes”*



way better than FalseCrypt

Does Not Protect Against

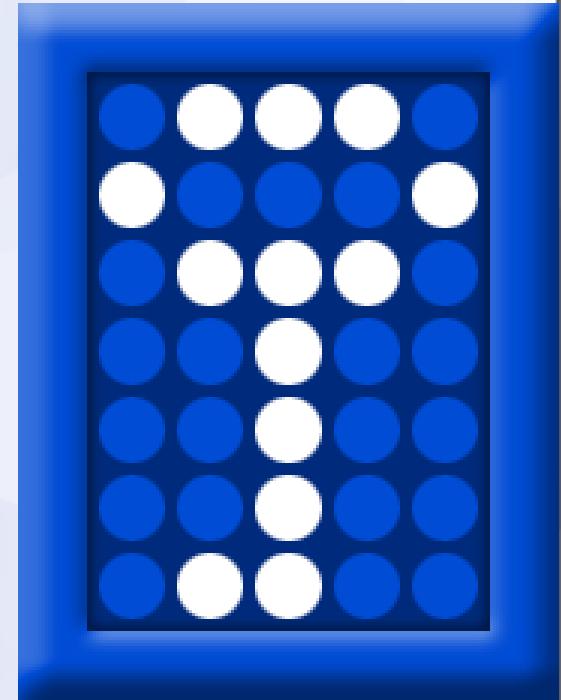
- *Misplaced trust*
- *Evil maid attacks*
- *User error*
- *Swap/cold boot attacks*
- *Rubber-hose attack*



way better than FalseCrypt

“Full-disk Encryption”

- *Immune to swap/recovery attacks*
- *Overall much more secure*
- *Slightly slower than folder encryption*



way better than FalseCrypt

TRUECRYPT

F R E E O P E N - S O U R C E O N - T H E - F L Y E N C R Y P T I O N

Home Documentation Downloads News Future History Screenshots Donations FAQ Forum Contact

TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

News

• 2012-02-07
TrueCrypt 7.1a
Released

• 2011-09-01
TrueCrypt 7.1
Released

• 2010-09-06
TrueCrypt 7.0a
Released

• 2010-07-19
TrueCrypt 7.0
Released

• 2009-11-23
TrueCrypt 6.3a
Released

[News Archive]

Please consider making a donation.



[Donate Now >>](#)

[Make a Donation](#)

Main Features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).
- Encryption is **automatic, real-time** (on-the-fly) and **transparent**.

TrueCrypt - Free Open-Source On-The-Fly Disk Encryption Software for Windows 7/Vista/XP , Mac OS X and Linux - Downloads - Mozilla Firefox

File Edit View Bookmarks Tools Help

TrueCrypt - Free Open-Source On-The-Fly D... +

www.truecrypt.org/downloads gpg4win gnu privacy assistant

List of supported versions of operating systems • Legal notices

Windows 7/Vista/XP/2000

Download TrueCrypt Setup 7.1a.exe (3.3 MB) PGP Signature

Mac OS X

Download .dmg package PGP Signature

Linux

(Select a package) Download .tar.gz containing an executable setup file PGP Signature

What are PGP signatures?

More Downloads

[Source code, language packs, past versions, public key](#)

TrueCrypt Setup 7.1a



Wizard Mode

Select one of the modes. If you are not sure which to select, use the default mode.



Install

Select this option if you want to install TrueCrypt on this system.

Extract

If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).

TrueCrypt Installer



Help

< Back

Next >

Cancel

TrueCrypt Setup 7.1a

Setup Options

Here you can set various options to control the installation process.



Please select or type the location where you want to install the TrueCrypt program files. If the specified folder does not exist, it will be automatically created.

C:\Program Files\TrueCrypt\

Browse...

- Install for all users
- Add TrueCrypt to Start menu
- Add TrueCrypt icon to desktop
- Associate the .tc file extension with TrueCrypt
- Create System Restore point



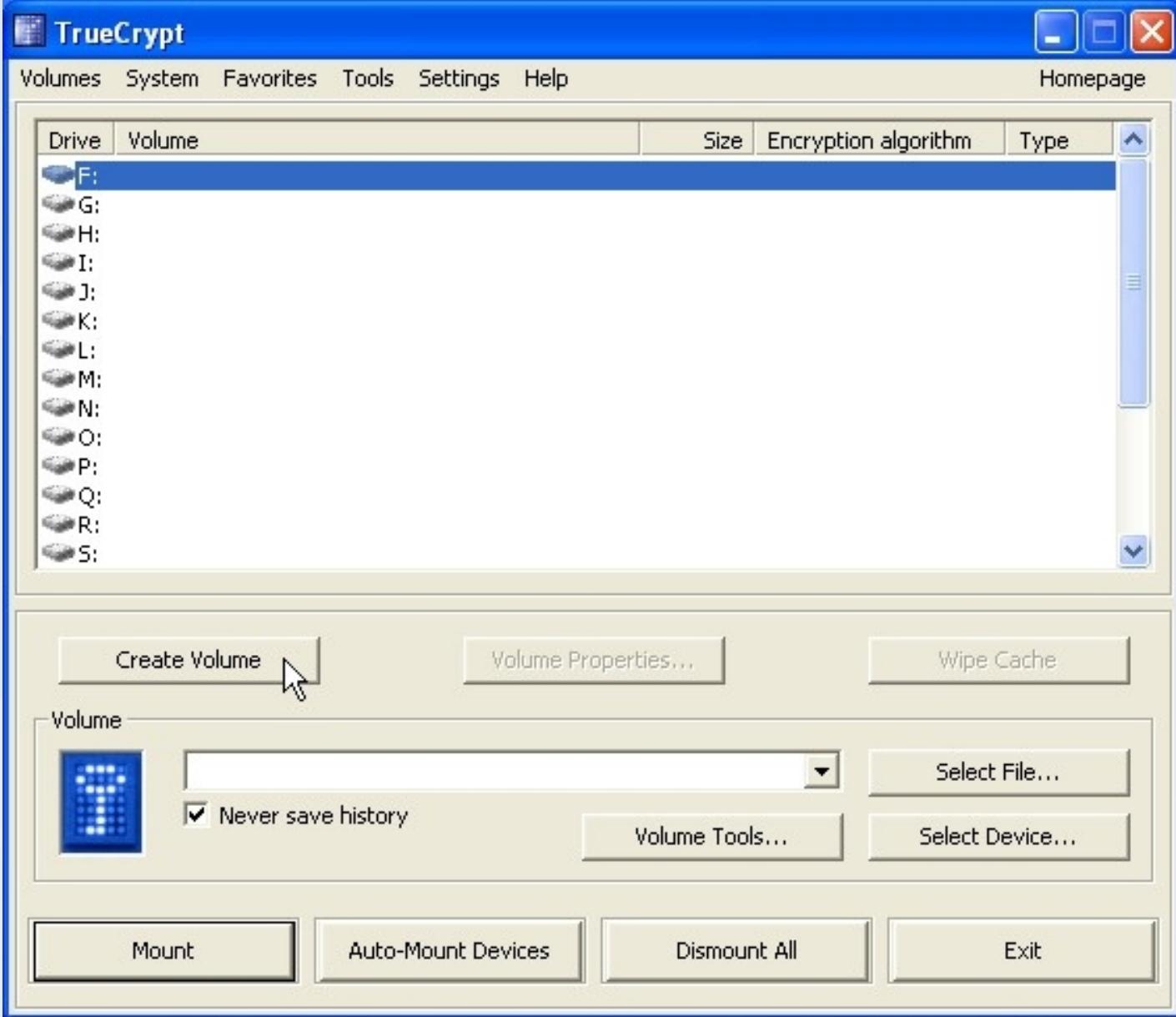
TrueCrypt Installer

Help

< Back

Install

Cancel



TrueCrypt Volume Creation Wizard



TrueCrypt Volume Creation Wizard

Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

[More information](#)

Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

[More information about system encryption](#)

Help

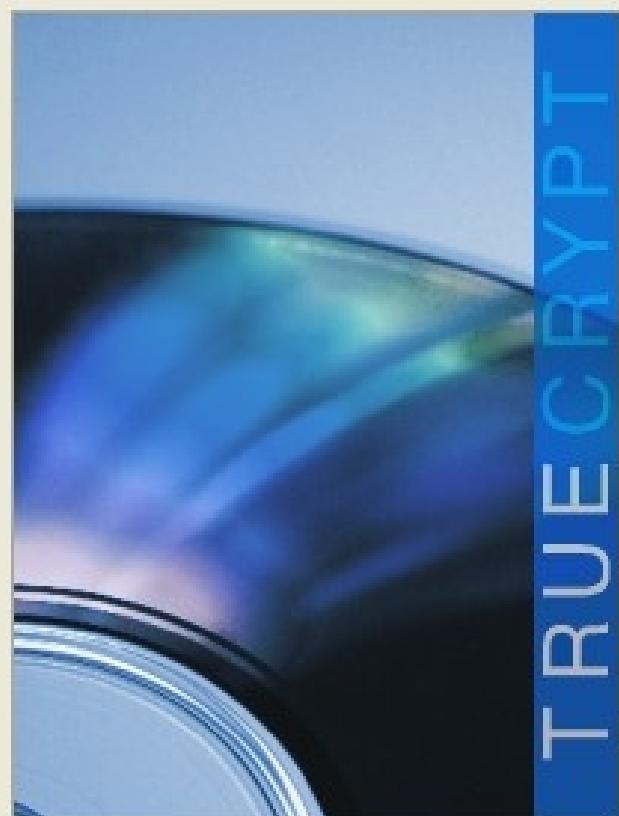
< Back



Next >

Cancel

TrueCrypt Volume Creation Wizard



Volume Type

Standard TrueCrypt volume

Select this option if you want to create a normal TrueCrypt volume.

Hidden TrueCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

[More information about hidden volumes](#)

Help

< Back

Nex>

Cancel

TrueCrypt Volume Creation Wizard

Volume Location

Select File... 

Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Help

< Back

Next >

Cancel

Specify Path and File Name



Save in:

user



My Recent
Documents



Desktop



My Documents



My Computer



My Network
Places

.kde

.tilemill

AppData

Desktop

Documents

Favorites

My Documents

Start Menu

UserData

tilemill

File name:

encrypted.file

Save

Save as type:

All Files (*.*)

Cancel



TrueCrypt Volume Creation Wizard



Volume Location

C:\Documents and Settings\user\Desktop

Select File...

Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Help

< Back

Next >

Cancel

Specify Path and File Name



Save in:



user



My Recent
Documents



Desktop



My Documents



My Computer



My Network
Places



.kde



.tilemill



AppData



Desktop



Documents



Favorites



My Documents



Start Menu



User Data



tilemill

File name:

encrypted.file

Save

Save as type:

All Files (*.*)

Cancel



Encryption Options

Encryption Algorithm

AES



Test

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

[More information on AES](#)

Benchmark

Hash Algorithm

RIPEMD-160



[Information on hash algorithms](#)

Help

< Back

Next >

Cancel



TrueCrypt Volume Creation Wizard



Volume Size

100

KB

MB

GB

Free space on drive C:\ is 9.98 GB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KB.
The minimum possible size of an NTFS volume is 3792 KB.

Help

< Back

Next >

Cancel

TrueCrypt Volume Creation Wizard

Volume Password

Password: *****

Confirm: *****

Use keyfiles

Keyfiles...

Display password

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

Help

< Back

Next >

Cancel

TrueCrypt Volume Creation Wizard



Volume Format

Options

Filesystem **NTFS** Cluster Default Dynamic

Random Pool: *****

Header Key: *****

Master Key: *****



Abort

Done

Speed

Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Help

< Back

Format

Cancel

TrueCrypt



Volumes System Favorites Tools Settings Help

Homepage

| Drive | Volume | Size | Encryption algorithm | Type |
|-------|--------|------|----------------------|------|
| F: | | | | |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | | | | |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| R: | | | | |
| S: | | | | |

Create Volume **Volume Properties...** **Wipe Cache**

Volume

 Never save history

Mount **Auto-Mount Devices** **Dismount All** **Exit**

Select a TrueCrypt Volume



Look in:

Desktop



My Recent Documents



Desktop



My Documents



My Computer



My Network Places

My Documents

My Computer

My Network Places

Mozilla Firefox

Mozilla Thunderbird

OpenOffice.org 3.2

TrueCrypt

encrypted_file

secret

secret.txt

File name:

encrypted

Open

Files of type:

All Files (*.*)

Cancel

TrueCrypt



Volumes System Favorites Tools Settings Help

Homepage

| Drive | Volume | Size | Encryption algorithm | Type |
|-------|--------|------|----------------------|------|
| ... | F: | | | |
| ... | G: | | | |
| ... | H: | | | |
| ... | I: | | | |
| ... | J: | | | |
| ... | K: | | | |
| ... | L: | | | |
| ... | M: | | | |
| ... | N: | | | |
| ... | O: | | | |
| ... | P: | | | |
| ... | Q: | | | |
| ... | R: | | | |
| ... | S: | | | |

Create Volume

Volume Properties...

Wipe Cache

Volume



C:\Documents and Settings\user\Desktop\encrypted.file

Select File...

Never save history

Volume Tools...

Select Device...

Mount

Auto-Mount Devices

Dismount All

Exit

Enter password for C:\Documents and Settings\...\encrypted.file

Password: *****

OK

Cancel

Cache passwords and keyfiles in memory

Display password

Use keyfiles

Keyfiles...

Mount Options...

TrueCrypt

Volumes System Favorites Tools Settings Help

Homepage

| Drive | Volume | Size | Encryption algorithm | Type |
|-------|---|-------|----------------------|--------|
| F: | C:\Documents and Settings\user\Desktop\encrypted.file | 99 MB | AES | Normal |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | | | | |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| R: | | | | |
| S: | | | | |



Create Volume

Volume Properties...

Wipe Cache

Volume



C:\Documents and Settings\user\Desktop\encrypted.file

Select File...

Never save history

Volume Tools...

Select Device...

Dismount

Auto-Mount Devices

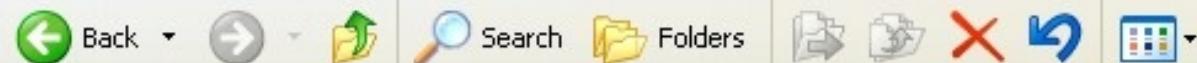
Dismount All

Exit

My Computer



File Edit View Favorites Tools Help



Files Stored on This Computer



Shared Documents



user's Documents

Hard Disk Drives



Local Disk (C:)



Local Disk (F:)



Devices with Removable Storage



CD Drive (D:)

Network Drives



vm on 'vboxsrv' (E:)

TrueCrypt Volume Creation Wizard



TrueCrypt Volume Creation Wizard

Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

[More information](#)

Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

[More information about system encryption](#)

Help

< Back

Next >

Cancel



Type of System Encryption

Normal

Select this option if you merely want to encrypt the system partition or the entire system drive.

Hidden

It may happen that you are forced by somebody to decrypt the operating system. There are many situations where you cannot refuse to do so (for example, due to extortion). If you select this option, you will create a hidden operating system whose existence should be impossible to prove (provided that certain guidelines are followed). Thus, you will not have to decrypt or reveal the password to the hidden operating system. For a detailed explanation, please click the link below.

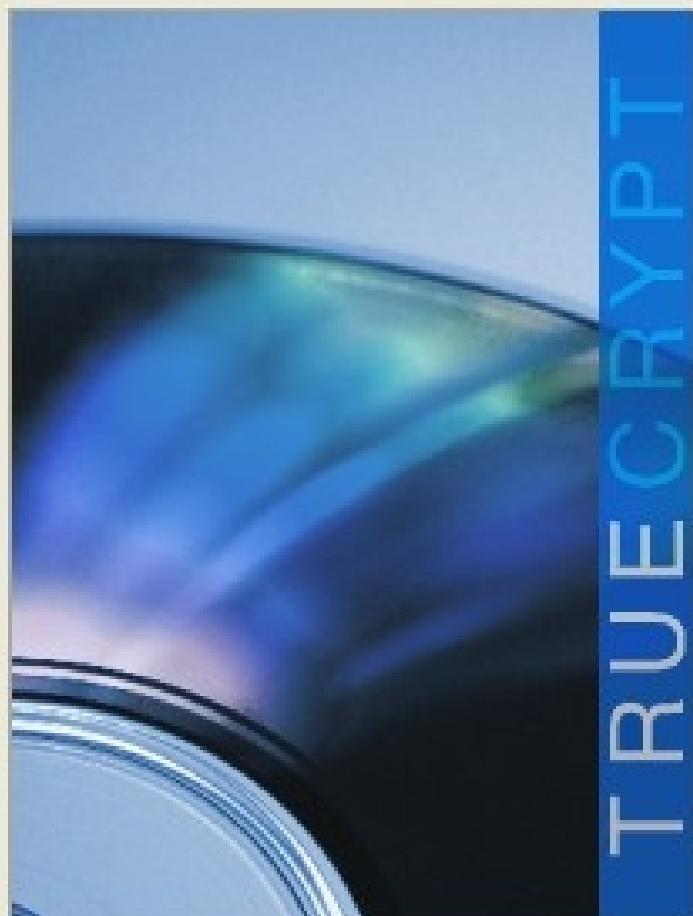
[More information](#)

Help

< Back

Next >

Cancel



Area to Encrypt

Encrypt the Windows system partition

Select this option to encrypt the partition where the currently running Windows operating system is installed.

Encrypt the whole drive

Select this option if you want to encrypt the entire drive on which the currently running Windows system is installed. The whole drive, including all its partitions, will be encrypted except the first track where the TrueCrypt Boot Loader will reside. Anyone who wants to access a system installed on the drive, or files stored on the drive, will need to enter the correct password each time before the system starts. This option cannot be used to encrypt a secondary or external drive if Windows is not installed on it and does not boot from it.

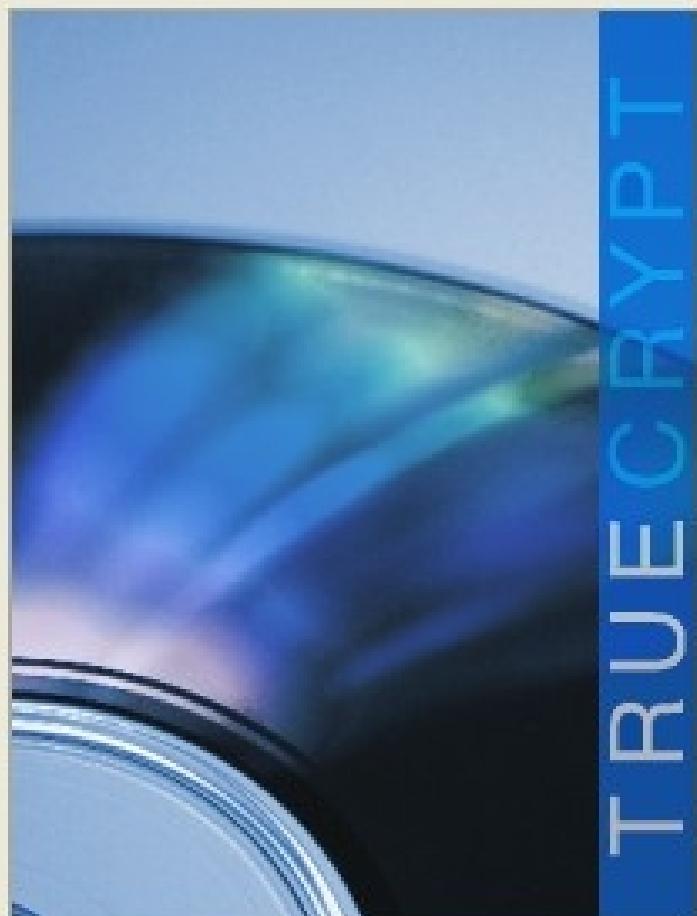


Help

< Back

Next >

Cancel



Encryption of Host Protected Area

Yes

No



At the end of many drives, there is an area that is normally hidden from the operating system (such areas are usually referred to as Host Protected Areas). However, some programs can read and write data from/to such areas.

WARNING: Some computer manufacturers may use such areas to store tools and data for RAID, system recovery, system setup, diagnostic, or other purposes. If such tools or data must be accessible before booting, the hidden area should NOT be encrypted (choose 'No' above).

Do you want TrueCrypt to detect and encrypt such a hidden area (if any) at the end of the system drive?

Help

< Back

Next >

Cancel

Single-boot

Select this option if there is only one operating system installed on this computer (even if it has multiple users).

Multi-boot



Select this option if there are two or more operating systems installed on this computer.

For example:

- Windows XP and Windows XP
- Windows XP and Windows Vista
- Windows and Mac OS X
- Windows and Linux
- Windows, Linux and Mac OS X

Help

< Back

Next >

Cancel



Rescue Disk

Before you can encrypt the partition/drive, you must create a TrueCrypt Rescue Disk (TRD), which serves the following purposes:

- If the TrueCrypt Boot Loader, master key, or other critical data gets damaged, the TRD allows you to restore it (note, however, that you will still have to enter the correct password then).
- If Windows gets damaged and cannot start, the TRD allows you to permanently decrypt the partition/drive before Windows starts.
- The TRD will contain a backup of the present content of the first drive track (which typically contains a system loader or boot manager) and will allow you to restore it if necessary.

The TrueCrypt Rescue Disk ISO image will be created in the location specified below.



TrueCrypt Volume Creation Wizard



Rescue Disk Recording

The Rescue Disk image has been created and stored in this file:
C:\Documents and Settings\user\Desktop\rescuedisk

Now you need to burn it to a CD or DVD.

IMPORTANT: Note that the file must be written to the CD/DVD as an ISO disk image (not as an individual file). For information on how to do so, please refer to the documentation of your CD/DVD recording software. If you do not have any CD/DVD recording software that can write the ISO disk image to a CD/DVD, click the link below to download such free software.

After you burn the Rescue Disk, click Next to verify that it has been correctly burned.

[Download CD/DVD recording software](#)

Help

< Back

Next >

Cancel



Rescue Disk Verified

The TrueCrypt Rescue Disk has been successfully verified. Please remove it from the drive now and store it in a safe place.

Click Next to continue.

[Help](#)[<< Back](#)[Next >](#)[Cancel](#)



Wipe Mode

Wipe mode: ▾

On some types of storage media, when data is overwritten with other data, it may be possible to recover the overwritten data using techniques such as magnetic force microscopy. This also applies to data that are overwritten with their encrypted form (which happens when TrueCrypt initially encrypts an unencrypted partition or drive). According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwriting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use such techniques to recover the data you intend encrypt, you may want to select one of the wipe modes (existing data will NOT be lost). Note that wiping will NOT be performed after the partition/drive is encrypted. When the partition/drive is fully encrypted, no unencrypted data is written to it. Any data being written to it is first encrypted on the fly in memory and only then is the (encrypted) data written to the disk.

Help

< Back

Next >

Cancel



System Encryption Pretest



Before encrypting your system partition or drive, TrueCrypt needs to verify that everything works correctly.

After you click Test, all the necessary components (for example, the pre-boot authentication component, i.e. the TrueCrypt Boot Loader) will be installed and your computer will be restarted. Then you will have to enter your password in the TrueCrypt Boot Loader screen that will appear before Windows starts. After Windows starts, you will be automatically informed about the result of this pretest.

The following device will be modified: Drive #0

If you click Cancel now, nothing will be installed and the pretest will not be performed.



Help

< Back

Test

Cancel



Pretest Completed

The pretest has been successfully completed.

WARNING: Please note that if power supply is suddenly interrupted while encrypting existing data in place, or when the operating system crashes due to a software error or hardware malfunction while TrueCrypt is encrypting existing data in place, portions of the data will be corrupted or lost. Therefore, before you start encrypting, please make sure that you have backup copies of the files you want to encrypt. If you do not, please back up the files now (you can click Defer, back up the files, then run TrueCrypt again anytime, and select 'System' > 'Resume Interrupted Process' to start encrypting).

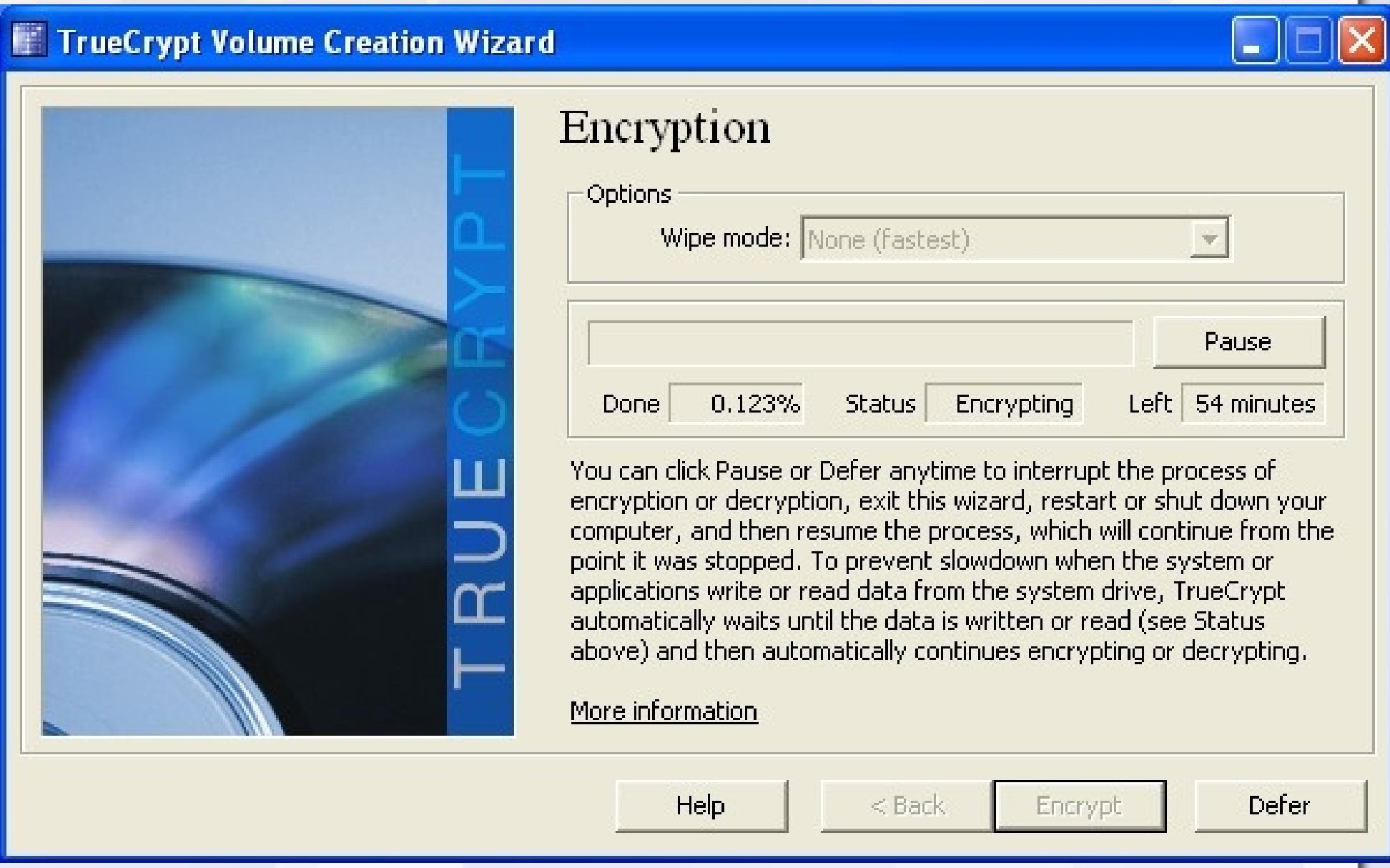
When ready, click Encrypt to start encrypting.

Help

< Back

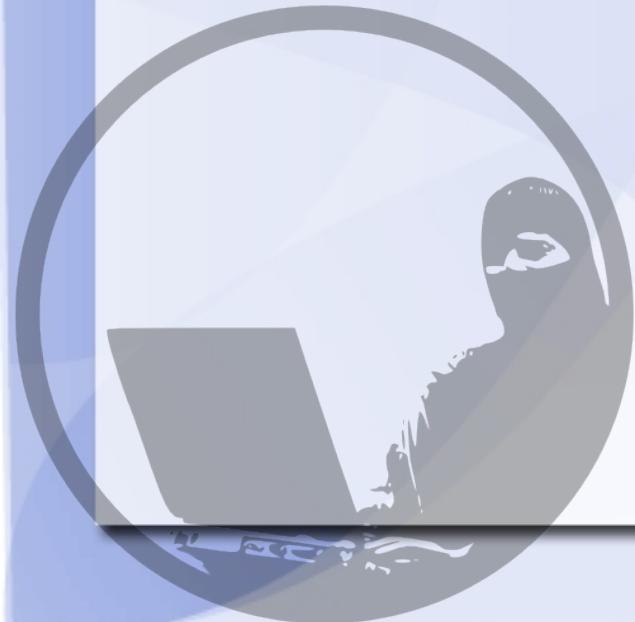
Encrypt

Defer



PGP Email Encryption

- *Cross-platform*
- *Works best with email clients*
- *Lots of moving parts*
- *Long-standing, open-source solution*
- *Can encrypt emails and files*



Nothing to see here

Protects Against

- *Unauthenticated conversations*
- *Adversary knowing what you are saying (body & attachment)*
- *Seizure from your computer or on the wire*



Nothing to see here

Does Not Protect Against

- *Adversary knowing who you are/are talking to*
- *Misplaced trust*
- *User error*
- *Swap/cold boot attacks*
- *Rubber-hose attack*



Nothing to see here



Max is sending an email encrypted with the Alle's public key

Encrypted connection
Can not be decoded by others

Alle's public key



Encrypted email



Encrypted connection
Can not be decoded by others

Alle's private key

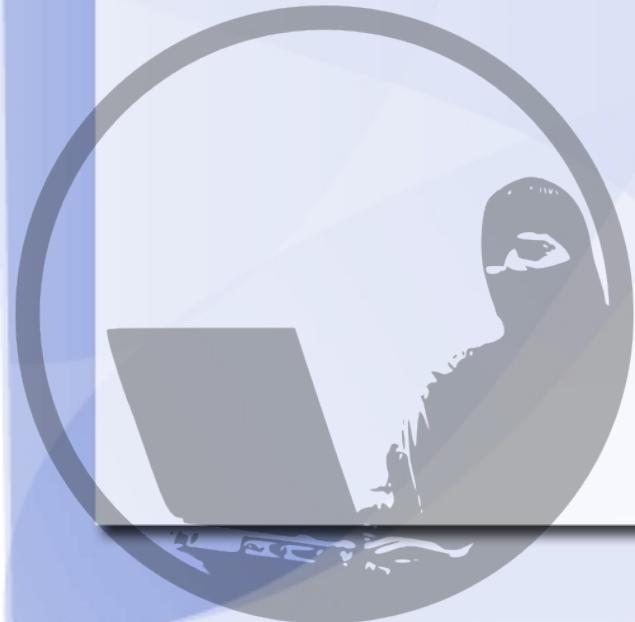


Alle has received the email from Max and decripts it with his own private key



Choosing a Secure Passphrase

- *Unique*
- *Letters, numbers, special characters*
- *It's a phrase, not a word*
- *Th1s 1s n0t s3cur3*



Nothing to see here

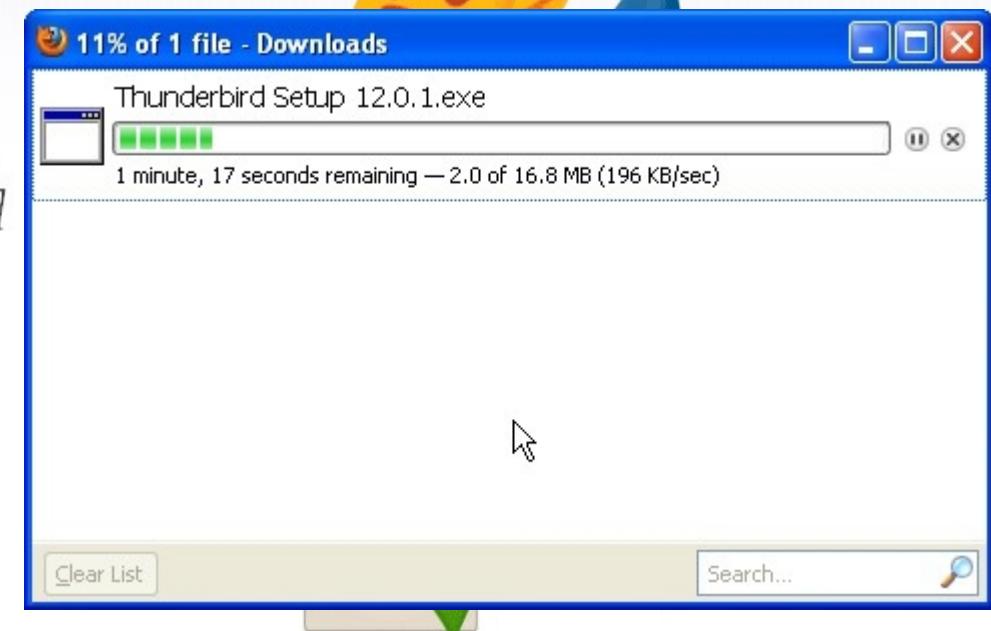
mozilla

Software made to make email easier.

Thunderbird is a free email application that's easy to set up and customize - and it's loaded with great features!



[Release Notes - Other Systems & Languages](#)



[Features](#) | [Add-Ons](#) | [Support](#) | [Community](#) | [Organizations](#) | [About](#)

[Privacy Policy](#) | [Legal Notices](#)

Copyright © 2005-2012 Mozilla. All rights reserved.



Welcome to the Mozilla Thunderbird Setup Wizard

This wizard will guide you through the installation of Mozilla Thunderbird.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

A mouse cursor icon pointing to the 'Next >' button.

Cancel

Setup Type

Choose setup options



Choose the type of setup you prefer, then click Next.

Standard

Thunderbird will be installed with the most common options.

Custom

You may choose individual options to be installed. Recommended for experienced users.



Use Thunderbird as my default mail application

< Back

Next >

Cancel

Summary

Ready to start installing Thunderbird



Thunderbird will be installed to the following location:

C:\Program Files\Mozilla Thunderbird

Thunderbird will be set as your default mail application.

Click Install to continue.



< Back

Install

Cancel



Completing the Mozilla Thunderbird Setup Wizard

Mozilla Thunderbird has been installed on your computer.

Click Finish to close this wizard.



Launch Mozilla Thunderbird now

< Back

Finish

Cancel

Mail Account Setup



Your name:

Your name, as shown to others

Email address:

Password:

Remember password



[Continue](#)

[Cancel](#)

Mail Account Setup



Your name: Super Mc. Secret

Your name, as shown to others

Email address: hackblocworkshop@gmail.com

Password: ██████████

Remember password

Configuration found in Mozilla ISP database

IMAP (remote folders) POP3 (keep mail on your computer)

Incoming: IMAP, imap.googlemail.com, SSL

Outgoing: SMTP, smtp.googlemail.com, SSL



Username: hackblocworkshop@gmail.com

[Manual config](#)

Create Account

[Cancel](#)

Inbox - Mozilla Thunderbird

File Edit View Go Message Tools Help

Inbox

Get Mail Write Address Book Tag Quick Filter Search... <Ctrl+K>

hackblocwor...p@gmail.com

Inbox (3)

[Gmail] Drafts Sent Mail All Mail Spam Trash Starred Personal Receipts Travel Work

Local Folders

Quick Filter: • ★ ☰ Filter these messages... <Ctrl+Shift+K>

| Subject | From | Date |
|--|------------|----------|
| ★ Get Gmail on your mobile phone | Gmail Team | 12:13 AM |
| ★ Import your contacts and old email | Gmail Team | 12:13 AM |
| ★ Customize Gmail with colors and themes | Gmail Team | 12:13 AM |

Welcome to  Thunderbird

 Thunderbird Contributors: QA and Development

When the Thunderbird team recently started talking about how to increase the size of the Thunderbird contributor community, we thought that one interesting thing we could do was to describe the daily life of members of the Thunderbird team. In this post, we introduce readers to Thunderbird's quality assurance and development activities, and link to profiles of Ludo, our QA Lead and David, Thunderbird Architect. In these profiles we describe the activities and

Mozilla Thunderbird is free and open source software from the non-profit Mozilla Foundation.

Know your rights... Unread: 3 Total: 3

[About Gpg4win](#)[Documentation](#)[Community](#)[Support](#)[Donate](#)

English | Deutsch

[Download
Gpg4win 2.1.0](#)[Change History - Check integrity](#)

News

2012-05-04

[**Gpg4win 2.1.1 Beta released**](#)

2011-03-15

[**Gpg4win 2.1.0 released**](#)[Older messages in news archive.](#)

Gpg4win - a secure solution...

... for file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

[Discover Gpg4win](#)[Getting started](#)[Join the community](#)

File Edit View History Bookmarks Tools Help

Gpg4win - Download Gpg4win



gpg4win.org/download.html



Google



- README

Gpg4win 2.1.0

You can download the full version (including the Gpg4win compendium) of Gpg4win 2.1.0 here:

Gpg4win 2.1.0



Size: 38 MByte | Released: 2011-03-15

- OpenPGP signatur (for gpg4win-2.1.0.exe)
- SHA1 checksum (for gpg4win-2.1.0.exe):
f619313cb42241d6837d20d24a814b81a1fe7f6d gpg4win-2.1.0.exe
- Change History
- Sources and other Gpg4win-2.1.0 variants:
 - Full version but *without* Kleopatra and manuals:

Gpg4win-Light 2.1.0

Size: 15 MByte

- OpenPGP signatur (for gpg4win-light-2.1.0.exe)
- gpg4win-2.1.0.tar.bz2 (source code package); Size: 5 MByte
- All versions and OpenPGP signatures: files.gpg4win.org.

Gpg4win 2.1.0 contains:

GnuPG 2.0.17
Kleopatra 2.1.0 (2011-02-04)
GPA 0.9.1-svn1024
GpgOL 1.1.2
GpgEX 0.9.7
Claws Mail 3.7.8cvs47
Kompendium (de) 3.0.0
Compendium (en) 3.0.0-beta1



Choose Components

Choose which features of Gpg4win you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- GnuPG
- Kleopatra
- GPA
- GpgOL
- GpgEX
- Claws-Mail
- Gpg4win Compendium



Description

GNU Privacy Assistant

Space required: 104.7MB



Define trustable root certificates

S/MIME configuration

Gpg4win needs a list of root certificates which you trust.

To avoid that each user must search and install the required root certificates, and also check and authenticate the trustworthiness of the same, it is useful to install a system-wide default of the most important root certificates:

1. Store the root certificates

Copy root certificate file to:

Therewith you can use S/MIME, the configuration is stringently required. Skip this configuration only if you don't want to use S/MIME.

Root certificate defined or skip configuration

Nullsoft Install System v2.46-2

< Back

Next >

Cancel

Inbox - Mozilla Thunderbird

File Edit View Go Message Tools Help

Inbox

Get Mail Write Add

hackblocwor...p@gmail.com

Inbox (3)

[Gmail]

- Drafts
- Sent Mail
- All Mail
- Spam
- Trash
- Important
- Starred
- Personal
- Receipts
- Travel
- Work

Local Folders

Address Book Ctrl+Shift+B

Saved Files Ctrl+J

Add-ons

Test Pilot

Activity Manager

Message Filters...

Run Filters on Folder

Run Filters on Message

Run Junk Mail Controls on Folder

Delete Mail Marked as Junk in Folder

Import...

Error Console

Account Settings...

Options...

Search... <Ctrl+K>

Filter these messages... <Ctrl+Shift+K>

From Date

mobile phone 12:13 AM

and old email 12:13 AM

colors and themes 12:13 AM

Would you like to help improve Mozilla Thunderbird by automatically reporting memory usage, performance, and responsiveness to Mozilla? [Learn More](#)

Yes No

Unread: 3 Total: 3

Add-ons Manager - Mozilla Thunderbird

File Edit View Go Message Tools Help

Inbox Add-ons Manager

enigmail

Name Last Updated Best match

Search: My Add-ons Available Add-ons

Enigmail 1.4.1 Friday, April 20, 2012

ENIG MAIL OpenPGP message encryption and authentication for Thunderbird and SeaMonkey. [More](#)

Install

iLeopard Mail 3.2.6 Monday, August 1, 2011

It is a Theme of the Mac Leopard-style which did iLeopard in a model. [More](#)

Install this add-on

Install

Display mailing list header 0.3.2 Saturday, April 21, 2007

This extension implements RFC 2369 for Thunderbird: Special mailing list header fields in the mail are parsed, and the links are displayed in the extended header view. You can click th... [More](#)

Install

Leopard Mail-Default-Graphite 3.2.6 Monday, August 02, 2010

This theme is the skin which can change your Thunderbird like LeopardMail. [More](#)

Install

Leopard Mail-Default-Aqua 3.2.6 Monday, August 02, 2010

This theme is the skin which can change your Thunderbird like LeopardMail. [More](#)

Install

Newsgroup Links 0.1.1 Monday, March 05, 2007

Displays a link to the Google groups url of a newsgroup post, and an option to copy it. [More](#)

Install

Would you like to help improve Mozilla Thunderbird by automatically reporting memory usage, performance, and responsiveness to Mozilla? [Learn More](#)

Yes No

The screenshot shows the Mozilla Thunderbird Add-ons Manager window. On the left, there's a sidebar with icons for Inbox, Search, Get Add-ons, Extensions, Appearance, and Plugins. The main area has a search bar at the top with the text 'enigmail'. Below the search bar, there are buttons for 'Name', 'Last Updated', and 'Best match'. The search results list several add-ons:

- Enigmail 1.4.1** (Available Add-ons) - Published on Friday, April 20, 2012. Description: OpenPGP message encryption and authentication for Thunderbird and SeaMonkey. Status: Available.
- iLeopard Mail 3.2.6** (Available Add-ons) - Published on Monday, August 1, 2011. Description: It is a Theme of the Mac Leopard-style which did iLeopard in a model. Status: Available.
- Display mailing list header 0.3.2** (Available Add-ons) - Published on Saturday, April 21, 2007. Description: This extension implements RFC 2369 for Thunderbird: Special mailing list header fields in the mail are parsed, and the links are displayed in the extended header view. You can click th... Status: Available.
- Leopard Mail-Default-Graphite 3.2.6** (Available Add-ons) - Published on Monday, August 02, 2010. Description: This theme is the skin which can change your Thunderbird like LeopardMail. Status: Available.
- Leopard Mail-Default-Aqua 3.2.6** (Available Add-ons) - Published on Monday, August 02, 2010. Description: This theme is the skin which can change your Thunderbird like LeopardMail. Status: Available.
- Newsgroup Links 0.1.1** (Available Add-ons) - Published on Monday, March 05, 2007. Description: Displays a link to the Google groups url of a newsgroup post, and an option to copy it. Status: Available.

At the bottom of the window, there's a message asking if the user wants to help improve Mozilla Thunderbird by automatically reporting memory usage, performance, and responsiveness to Mozilla, with 'Yes' and 'No' buttons.

Add-ons Manager - Mozilla Thunderbird

View Go Message Tools Help

 Add-ons Manager

X



enigmail



Name

Last Updated

Best match ▾

Search: My Add-ons Available Add-ons

✓ Enigmail will be installed after you restart Thunderbird. [Restart now](#) [Undo](#)



Enigmail 1.4.1

OpenPGP message encryption and authentication [More](#)

Friday, May 25, 2012



iLeopard Mail 3.2.6

Monday, August 02, 2010

[Install](#)



Display mailing list header 0.3.2

Saturday, April 21, 2007

[Install](#)



Leopard Mail-Default-Graphite 3.2.6

Monday, August 02, 2010

[Install](#)



Leopard Mail-Default-Aqua 3.2.6

Monday, August 02, 2010

[Install](#)

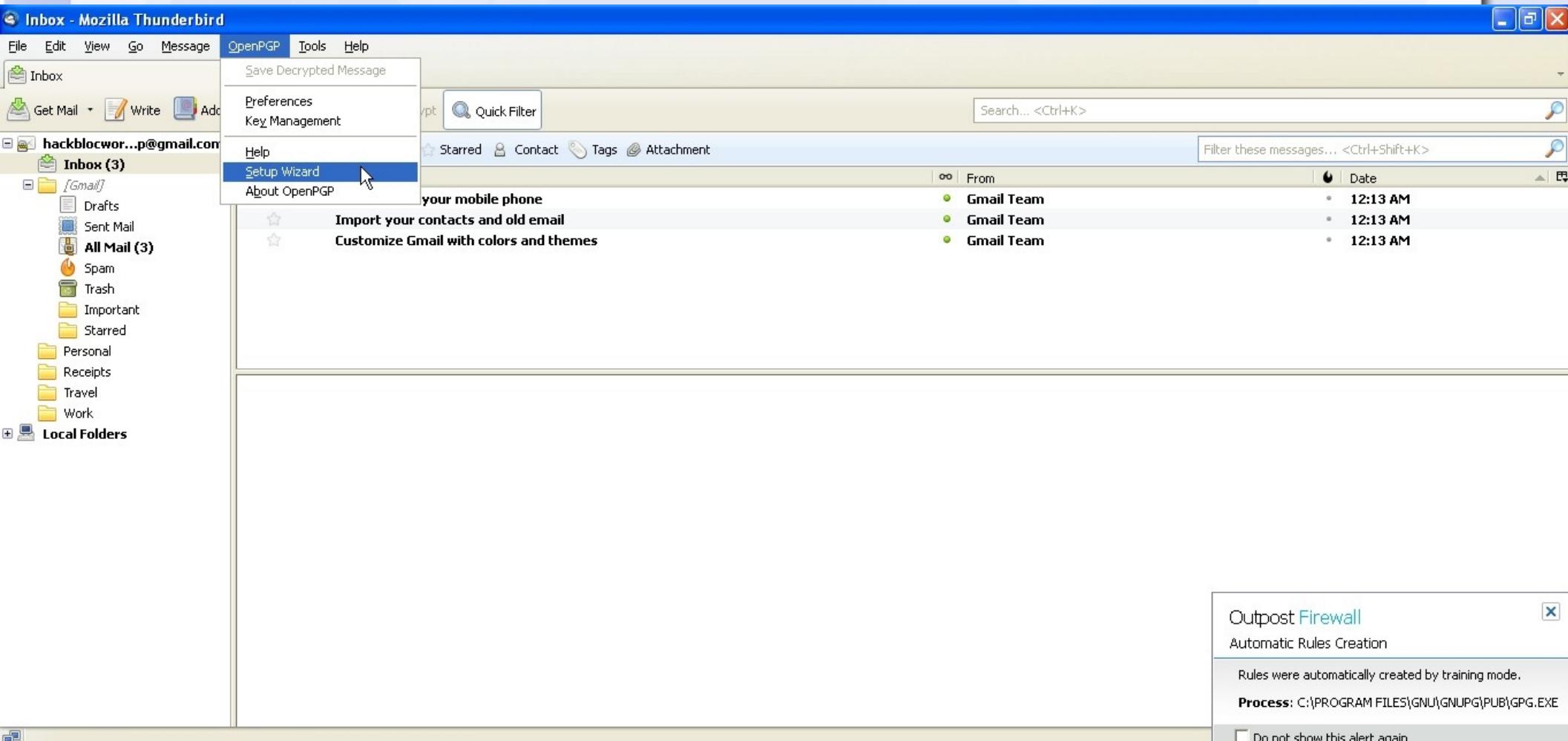


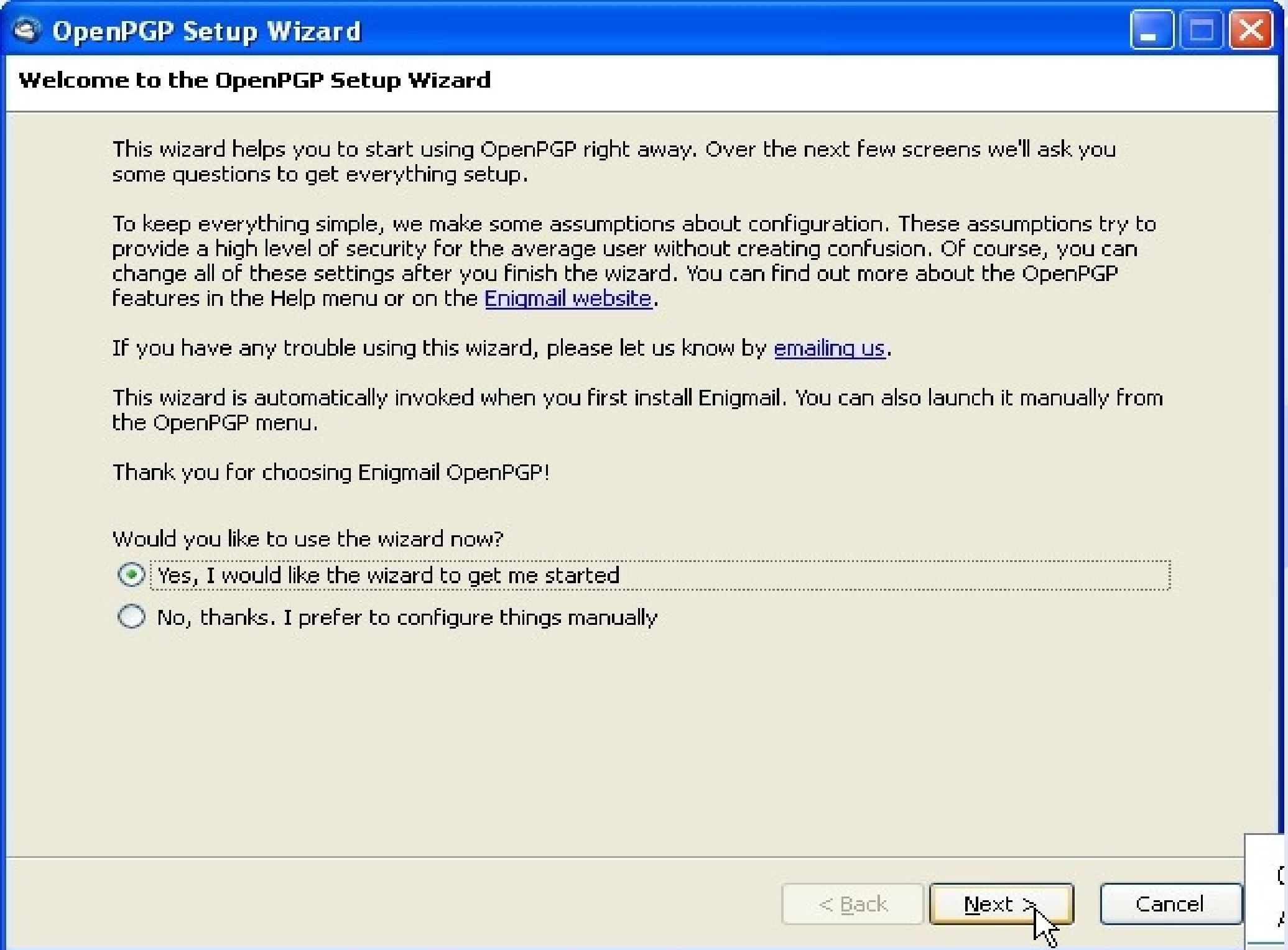
Newsgroup Links 0.1.1

Monday, March 05, 2007

[Install](#)

ocworkshop@gmail.com is up to date





OpenPGP Setup Wizard



Welcome to the OpenPGP Setup Wizard

This wizard helps you to start using OpenPGP right away. Over the next few screens we'll ask you some questions to get everything setup.

To keep everything simple, we make some assumptions about configuration. These assumptions try to provide a high level of security for the average user without creating confusion. Of course, you can change all of these settings after you finish the wizard. You can find out more about the OpenPGP features in the Help menu or on the [Enigmail website](#).

If you have any trouble using this wizard, please let us know by [emailing us](#).

This wizard is automatically invoked when you first install Enigmail. You can also launch it manually from the OpenPGP menu.

Thank you for choosing Enigmail OpenPGP!

Would you like to use the wizard now?

- Yes, I would like the wizard to get me started
- No, thanks. I prefer to configure things manually

< Back

Next >

Cancel



Encryption

Encrypt Your Outgoing Emails

OpenPGP allows you to encrypt your email messages and any attachments. Encryption is like putting a letter in an envelope. It makes things private. It's not just for "secret" messages, but for everything that you would not send on a postcard.

On a technical level, encryption works like a padlock that only the recipient has the key for. Unlike signing, to use encryption all the recipients of an email need to use OpenPGP. People need to give you their public key before you can send them encrypted email (the public key is the pad lock we were talking about).

Unless most of your communication partners have public keys, you should not enable encryption by default.

Shall your outgoing email be encrypted by default?

- Yes, I have public keys for most of my contacts
- No, I will create per-recipient rules for those that sent me their public key

< Back

Next >

Cancel

Preferences

Change Your Email Settings To Make OpenPGP Work More Reliably

This wizard can change your email settings to make sure there are no problems with signing and encrypting email on your machine. These setting changes are mostly technical stuff you will not notice, though one important thing is that email will be composed in plain text by default.

Do you want to change a few default settings to make OpenPGP work better on your machine?

Yes [Details ...](#)

No, thanks



< Back

Next >

Cancel



OpenPGP Setup Wizard



No OpenPGP Key Found

We could not find any OpenPGP Key

We could not find any OpenPGP key. Please select below if you want to create a new key pair or if you want to import an existing key.



I want to create a new key pair for signing and encrypting my email



I have existing public and private keys that I would like to import



< Back

Next >

Cancel

OpenPGP Setup Wizard



Summary

Confirm that the wizard shall now commit these changes

You are almost complete! If you click on the 'Next' button, the wizard will perform the following actions:

- Create a new 2048-bit OpenPGP key, valid for 5 years
- Activate OpenPGP for your email account
- Do not sign emails by default
- Do not encrypt emails by default
- Adjust all recommended application settings



< Back

Next >

Cancel

OpenPGP Setup Wizard



Summary

Confirm that the wizard shall now commit these changes

You are almost complete! If you click on the 'Next' button, the wizard will perform the following actions:

- Use the existing OpenPGP key ID 0E8FED008375E606 for signing
- Activate OpenPGP for your email account
- Do not sign emails by default
- Do not encrypt emails by default
- Adjust all recommended application settings

< Back

Next >

Cancel

Inbox - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Inbox

Get Mail Write Address Book Tag Decrypt Quick Filter Search... <Ctrl+K>

hackblocwor...p@gmail.com Quick Filter: • Unread ★ Starred Contact Tags Attachment Filter these messages... <Ctrl+Shift+K>

Inbox (3) Create a new message

| Subject | From | Date |
|--|------------|------------|
| ★ Get Gmail on your mobile phone | Gmail Team | • 12:13 AM |
| ★ Import your contacts and old email | Gmail Team | • 12:13 AM |
| ★ Customize Gmail with colors and themes | Gmail Team | • 12:13 AM |

[Gmail] Drafts Sent Mail All Mail (3) Spam Trash Important Starred Personal Receipts Travel Work Local Folders

Unread: 3 Total: 3

Write: THIS IS A TEST SUPER SECRET

File Edit View Options OpenPGP Tools Help

Send ABC Spelling Attach PGP OpenPGP S/MIME Save

From: Super Mc. Secret <hackblocworkshop@gmail.com> hackblocworkshop@gmail.com

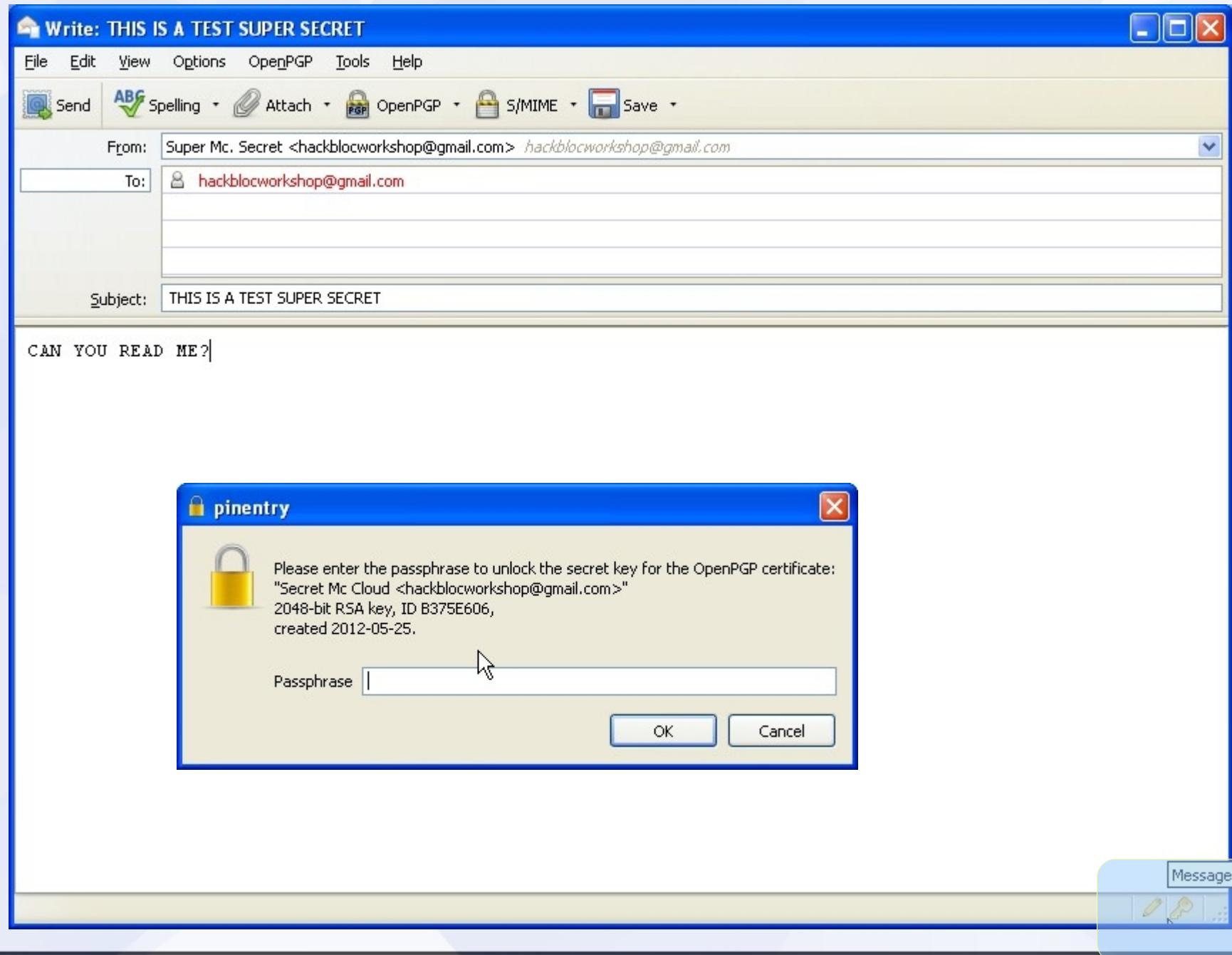
To: [hackblocworkshop@gmail.com](#)

Subject: THIS IS A TEST SUPER SECRET

CAN YOU READ ME?

Message





Write: THIS IS A TEST SUPER SECRET

File Edit View Options OpenPGP Tools Help



Spelling



OpenPGP



Save

From: Super Mc. Secret <hackblocworkshop@gmail.com> hackblocworkshop@gmail.com

To:

hackblocworkshop@gmail.com

Subject: THIS IS A TEST SUPER SECRET

-----BEGIN PGP MESSAGE-----

Charset: ISO-8859-1

Version: GnuPG v2.0.19 (Min

Comment: Using GnuPG with M

hQEAOXjpwQvxaENAQf+P9LxQcm

UTyBWVkwnZB8ud+41W2A28OgPHw

Qz8/+OI2pImKtvpl+udCrt0+o8Q

PyDd1TOHwDckWNSSnYS5AyqLLA1N

S0Z15fNM1VsSuOK1ko0umzYQ1PfpM+CAUnqKXM1zs+9uNWovcC5MGLouWjm1BW/a

faQmZHDe8cKU12EpoE7PoE2BPTqM6dU07vWzXeWGftLAvgFM04HIHgnYhoacvMC7

CT+x2rUPoifCTv7UJ4vrj8jZZccrHUI/OvzcXVOKL1EP9EB+Pp1G4ajXowiaNAb0

CrZxPTNcqP1cTMYzPIrzgSJ28lviakog5C1Ns1E7J/Laq75vkrN2bZSTP9D2v3HV

rhOG5rAa/TXgL7FY+pfJz6zzPrPfYHJuH6MpI2GOYPBNhyLL8YxMRTGee/+PdQ

id1p31M4STeEhZxho10h50x1NEBsAxG7cGfctckyuqpaB+OsnGS2gGL7GIgrEGu

tketcHPqj/sgU82uSTC+8y3u41K1FHW80hL9h01Gr3t1JdCddVnKCplEziZY6BQ1

adyaOtyF/7AJIM2hjev59cgsSiSWsx999CL01JhEDdFHyvYJhvoHRShYTC9EbeXx

LnpsePsd1v+YWP+cxeieSbrUoudrYtzBti67FzmtD70YELFVlunIkBhs9MfAsrDft

M7ENzmFf6ZpSFczTU39d/53VPKGT7N1NrmU86yr5dgU=

=LUcs

-----END PGP MESSAGE-----

Sending Messages - THIS IS A TEST SUPER SECRET

Status: Connected to smtp.googlemail.com...

Progress:



Cancel

Connected to smtp.googlemail.com...

Inbox - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Inbox

Get Mail Write Address Book Tag Decrypt Quick Filter

Search... <Ctrl+K>

hackblocwor...p@gmail.com

Inbox (4)

- [Gmail] Drafts
- Sent Mail
- All Mail (4)
- Spam
- Trash
- Important
- Starred
- Personal
- Receipts
- Travel
- Work

Local Folders

Quick Filter: • Unread ★ Starred Contact Tags Attachment

Filter these messages... <Ctrl+Shift+K>

| Subject | From | Date |
|--|------------------|------------|
| Get Gmail on your mobile phone | Gmail Team | • 12:13 AM |
| Import your contacts and old email | Gmail Team | • 12:13 AM |
| Customize Gmail with colors and themes | Gmail Team | • 12:13 AM |
| * THIS IS A TEST SUPER SECRET | Super Mc. Secret | • 12:24 AM |

hackblocworkshop@gmail.com received 1 new message

THIS IS A TEST SUPER SECRET Super Mc. Secret

-----BEGIN PGP MESSAGE----- Charset: ISO-8859-1 Version: GnuPG v2.0.19 (MingW32)...

Inbox - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Inbox

Get Mail Write Address Book Tag Decrypt Quick Filter Search... <Ctrl+K>

hackblocwor...p@gmail.com

Inbox (3)

- [Gmail] Drafts
- Sent Mail
- All Mail (4)
- Spam
- Trash
- Important
- Starred
- Personal
- Receipts
- Travel
- Work

Local Folders

Quick Filter: • Unread ★ Starred Contact Tags Attachment Filter these messages... <Ctrl+Shift+K>

| Subject | From | Date |
|--|------------------|----------|
| Get Gmail on your mobile phone | Gmail Team | 12:13 AM |
| Import your contacts and old email | Gmail Team | 12:13 AM |
| Customize Gmail with colors and themes | Gmail Team | 12:13 AM |
| THIS IS A TEST SUPER SECRET | Super Mc. Secret | 12:24 AM |

+ OpenPGP Decrypted message; Good signature from Secret Mc Cloud <hackblocworkshop@gmail.com>

From: Me ★
Subject: THIS IS A TEST SUPER SECRET
To: Me ★

Details ▾
Reply Forward Archive Junk Delete
12:24 AM
Other Actions ▾

CAN YOU READ ME?

Unread: 3 Total: 4

Write: Re: THIS IS A TEST SUPER SECRET

File Edit View Options OpenPGP Tools Help



ABC



Spelling



Attach



OpenPGP



S/MIME



Save

From: Super Mc. Secret <hackblocworkshop@gmail.com> hackblocworkshop@gmail.com

To:

Super Mc. Secret <hackblocworkshop@gmail.com>

Subject: Re: THIS IS A TEST SUPER SECRET

On 5/25/2012 12:24 AM, Super Mc. Secret wrote:

> CAN YOU READ ME?



Inbox - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Inbox

Get Mail Write Address Book Tag Decrypt Quick Filter Search... <Ctrl+K>

hackblocwor...p@gmail.com

Inbox (3)

[Gmail] Drafts Sent Mail All Mail (4) Spam Trash Important Starred Personal Receipts Travel Work Local Folders

Quick Filter: Unread Starred Contact Tags Attachment

Filter these messages... <Ctrl+Shift+K>

| Subject | From | Date |
|--|------------------|----------|
| Get Gmail on your mobile phone | Gmail Team | 12:13 AM |
| Import your contacts and old email | Gmail Team | 12:13 AM |
| Customize Gmail with colors and themes | Gmail Team | 12:13 AM |
| THIS IS A TEST SUPER SECRET | Super Mc. Secret | 12:24 AM |

OpenPGP Decrypted message; Good signature from Secret Mc Cloud <hackblocworkshop@gmail.com>

From Me ★
Subject Me
To Edit Contact...
Compose Message To
Copy Email Address
CAN
Create Filter From...
Create OpenPGP Rule from Address... []

Reply Forward Archive Junk Delete
12:24 AM Other Actions

Unread: 3 Total: 4

The screenshot shows the Mozilla Thunderbird interface with an open inbox window. The left sidebar displays a tree view of email accounts and local folders. The main pane shows four messages in the inbox, all from the 'Gmail Team'. One message is selected, revealing its content: 'Get Gmail on your mobile phone', 'Import your contacts and old email', 'Customize Gmail with colors and themes', and 'THIS IS A TEST SUPER SECRET'. Below the message list, a context menu is open over the recipient field 'Me' in the message header. The menu options include 'Edit Contact...', 'Compose Message To', 'Copy Email Address', 'CAN', 'Create Filter From...', and 'Create OpenPGP Rule from Address...'. The 'Create OpenPGP Rule from Address...' option is highlighted with a blue selection bar. The bottom status bar indicates there are 3 unread and 4 total messages.

OpenPGP - Recipient Settings



Set OpenPGP Rules for

(Separate several email
addresses with spaces)

Apply rule if recipient

Is exactly



one of the above addresses

Action

- Continue with next rule for the matching address
- Do not check further rules for the matching address
- Use the following OpenPGP keys:

(none - no encryption)

Select Key(s)...



Defaults for ...

Signing

Always



Encryption

Always



PGP/MIME

Yes, if selected in Message Composition



(Note: in case of conflicts, 'Never' overrules 'Always')

OK

Cancel

Help

Inbox - Mozilla Thunderbird

File Edit View Go Message OpenPGP Tools Help

Inbox Get Mail Write Add

hackblocwor...p@gmail.com

Inbox (2)

/Gmail

- Drafts
- Sent Mail
- All Mail (2)
- Spam
- Trash
- Important
- Starred
- Personal
- Receipts
- Travel
- Work

Local Folders

OpenPGP Tools Help

Save Decrypted Message

Preferences Key Management

Help Setup Wizard About OpenPGP

vpt Quick Filter

Starred Contact Tags Attachment

Search... <Ctrl+K>

Filter these messages... <Ctrl+Shift+K>

From Date

Gmail Team 12:13 AM

Gmail Team 12:13 AM

Gmail Team 12:13 AM

your mobile phone

Import your contacts and old email

Customize Gmail with colors and themes

From: Gmail Team <mailto:mail-noreply@google.com>

Subject: Customize Gmail with colors and themes

To: Me

12:13 AM Other Actions

To spice up your inbox with colors and themes, check out the Themes tab under Settings.

Customize Gmail » <https://mail.google.com/mail/#settings/themes>

Enjoy!

- The Gmail Team
[image: Themes thumbnails]

Please note that Themes are not available if you're using Internet Explorer 6.0. To take advantage of the latest Gmail features, please upgrade to a fully supported browser

http://support.google.com/mail/bin/answer.py?answer=6557&hl=en&utm_source=wel-eml&utm_medium=eml&utm_campaign=en

Deleted 1 message from Sent Mail Unread: 2 Total: 3

OpenPGP Key Management



File Edit View Keyserver Generate

Search for: work

Clear

Display All Keys by Default

Name

Key ID

+ Secret Mc Cloud <hackblocworkshop@gmail.com>

B375E606

Additional Tools of Interest

- *Etherpad*
- *SpiderOak, BTSync*
- *Privnote*
- *HackThisZine*
- *Linux + LUKS Encryption*
- *Mega.co.nz*
- *VPN and Proxy services*

