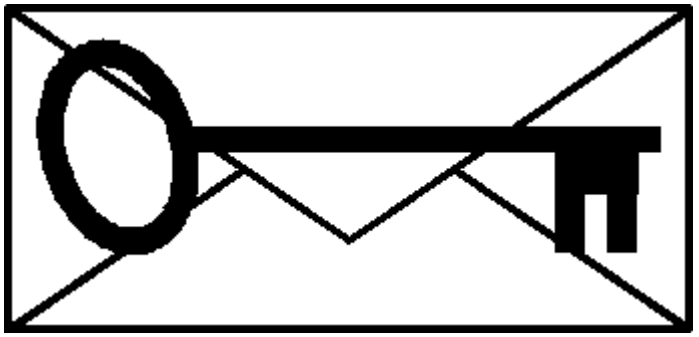
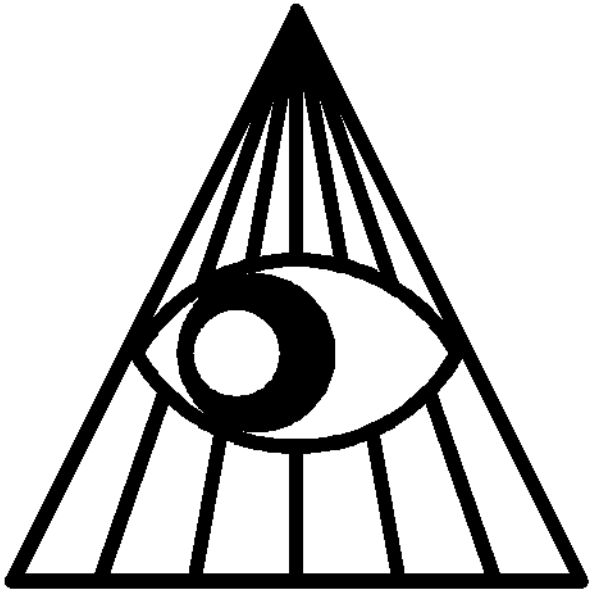
Total Encryption





Encryption?

~~Encryption?~~

Cryptography

single files

RAR

ZIP

Windows file encryption

holes

easy to crack

easy to crack
(in the past)

why?

encryption
not core feature

touchstone?

household name?

PGP

Pretty Good Privacy

Phil Zimmermann
1991

mail

Encryption/ Decryption

Signing/ Verification

proof of identity

1990’s

```
-----BEGIN PGP MESSAGE-----
Version: foo

hQIOA2US7SR8WYFzEAf+MSrImHD0Wq3HdxaPPPzj2yk50U1c0FD901HXlQROTyUv
8YGsig/y1vUFyJVtDU/cqgG0cDVAMLxpL24Mn/j/IQo9sJOeZGsEjCpu0r5T0F7E
OgH6GPejjQooFZldx6hOP9cpQmQpXJqH+QhbBgZCOWC+nBLEUoxX+K0qTpNhrFd+
EGxOrjkYOyhARd9H2oMcGGKhvZlJ9MMey3+tn/NSXrQ8Ulu/MG10xGnqvsd/nXDl
cqcRmRLojLJwJZ8QqgocVT+32lCMRZ/VrGPMo2SQHM5ipDHd3/X9KTf3n9C+estJ
NekGEKbE5GEBvJb7jbxg6CPv8ZrQM1z+Jq0GZs4b2Af/TTf4s59zMDC+CF2UR0NX
q5e+VDrKi2B1c51EhJEirqgcjbYodJIUrPE69MKkpOS2MbCBcAGkXRJHNf6XRJEW
OR6M0zPltejZLCLfpYo2ixfvFkB7QDDbiQYpxHn+8hrNTFdwFNjvYNhMOpdM+dxY
wOn1ZCwtLsmoG8l7QDLK6ZLAJ/ceY0lDmill3iFLATGsFl1xpauU4Jj7+5/E3Acm
kMM7Me7VOEg6dpLxZ86JZml4tQsygOg2WhzSjo3eheAbd7DywzzMtTEuB0orAR1P
0EnUgJ2ELwgh2LEiB/4bQxEM5+XyshYJd6kCoIVJyuVRo7YRf5POflcqGkviRr+s
nNLqAb3IMi1ya5jTCkSlPpGPF9ZC5vA2Sd0PIltdI3ueSAPWezA6iAmwXSyR/7nh
DXIQzLkhqvlxP6qqYrOxWRtD63DpuR2pA+7edDluD/B7bjw6s2S0ev5TLpbUTNSH
P4TSwC2G+SIjFPe/ehUw6DGHwZ4m2UMEdHv+EN7PNjjGclCvg9X0lkKm/B1L+UyQ
c+QTaU82wg/t3V408iPBMybrt/PIc8cqQhNQ+F9i9WjmrSGMpssyl+IBwV5gQxKe
5Ev6K/y3hBHJ5RkKTL5j/YF/LavalHbS7+FhgqLjNnX2DyBp7bvYIluRVobFexN9
...
iCI/OEI4PR8CwvzAy43o0Ezys1pN9K7WBcQrHoXBTyEuMFuJRPZkyZo0z4WUCehy
OJK0O2VJZiZSHPjNW6ch4Yl8YWfrMGM=
=Joo8
-----END PGP MESSAGE-----
```


$ pgp -d

2000

$

PGP Encryption Solutions

"PGP encryption technology delivers a solid security platform."

—Jon Allen, Information Security Officer, Baylor University

Solutions

Overview

PGP SDK

Solution Packages

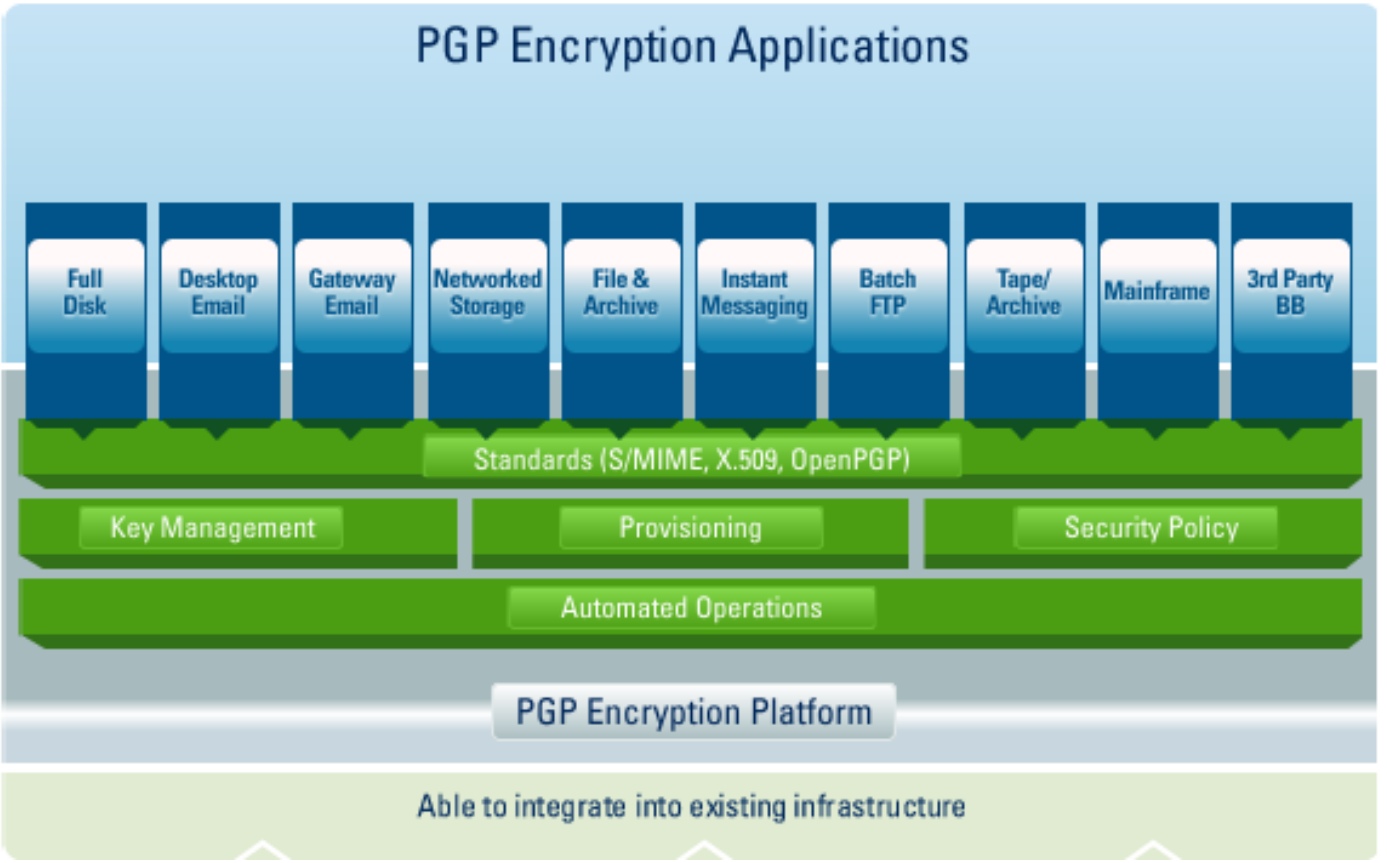
PGP Global Directory

Upgrades & Licensing

Feature Request Form

PGP Glossary

Contact Us



Solutions

- Total Protection
- Active Virus Defense
- Active VirusScan

Products

- Anti-spam
- Anti-spyware
- Anti-virus
- Data Protection
- Command Line Encryption
  - E-Business Server for OS/390
  - E-Business Server Partner Edition
  - E-Business Client
  - E-Business Server Native APIs
  - E-Business Server
- Host intrusion prevention
- Messaging and web security
- Mobile Security
- Network Access Control
- Network intrusion prevention
- Risk and compliance

McAfee E-Business Server

MCAFEE SYSTEM PROTECTION

Secure sensitive corporate assets anywhere in your enterprise

Automatically safeguard your sensitive corporate data with McAfee E-Business Server and industry-standard PGP 128-bit encryption and authentication. McAfee E-Business Server supports a variety of platforms and security certificates so you can exchange information safely with key business partners.

Datasheet

Benefits and Features | Description | System Requirements

Benefits:

- **Safeguard your valuable data**
  In storage, in transit, and during access, you can protect your assets from unauthorized use with robust PGP encryption
- **Encrypt files quickly and easily**
  Drag and drop files for automatic encryption, compression, data integrity, and authentication using

Features:

- **Industrial-strength encryption**
  E-Business Server uses the industry's strongest encryption algorithms, including Triple-DES CAST, IDEA, and the Twofish Cipher Algorithm
- **Embed encryption into applications**
  Your developers can quickly and easily embed encryption services into

How To Buy

Security is quick and easy with partners who help you find, acquire, and install our solutions.

- Find a partner
- Contact a sales representative

Useful Links

- Register software
- Free product trials

Resources

- White Paper: Send and store data securely over the internet

Demos and Tutorials

For more information on McAfee E-Business Server, please contact McAfee at ebssales@mcafee.com

IETF®

standardized

OpenPGP

OpenPGP
RFC 4880

in actual use


GnuPG

problem


$ gpg --decrypt

Enigmail


Zur Beachtung!
Beachte die Gebrauchsanleitung für die Chiffriermaschine (H. Dv. g. 13)
1. Zur Säuberung der Walzenkontakte alle Walzen mehrmals gegenseitig vor- und rückwärtsdrehen.
2. Zur Säuberung der Tastenkontakte sämtliche Tasten vor Einschaltung des Stromes mehrmals kräftig herunterdrücken und hochschnellen lassen, wobei eine Taste dauernd gedrückt bleibt.
3. Bei Einstellung der in den Fenstern sichtbaren Zeichen beachten, daß die Walzen richtig gerastet sind.
4. Die unverwechselbaren doppelpoligen Stecker sind bis zum Anschlag in ihre Buchsenpaare einzuführen.
Die vordere Halteklappe ist danach zu schließen, da sonst 3 Lampen zugleich aufleuchten können.
5. Leuchtet bei Tastendruck keine Lampe auf, so sind die Batterie, ihre Kontaktfedern, ihre Anschlüsse am Umschalter und der Umschalter zu prüfen.
6. Leuchten bei Tastendruck eine oder mehrere Lampen nicht auf, so sind die entsprechenden Lampen, die Kontakte unter ihnen, die Kabel der doppelpoligen Stecker, die Steckerbuchsen einschließlich ihrer Kurzschlußlasche, die Walzenkontakte, die Arbeitskontakte unter den jeweils gedrückten Tasten und die Ruhekontakte unter den mit ihnen korrespondierenden Tasten, zu prüfen und bei etwa vorhandenen Verschmutzungen und Oxydationen zu säubern. (Siehe auch Ziffer 2).
Von Maschine Nr. A 4388 ab dient zur Lampenprüfung die Ch-Taste.
Reihe am Steckerbrett und die Kabelprüflampe auf der linken Lampenfeldseite.
7. Walzenachse und Walzenbuchsen sind sauber zu halten und wie alle übrigen Lagerstellen hin und wieder mit harz- und säurefreiem Öl leicht einzufetten. Die festen Kontakte der Walzen sind alle 6–8 Wochen mit Polierpapier abzureiben.
Die Tastenkontakte, die Lampenkontakte und die Kurzschlußfläche sind vor Öl zu schützen.
8. Schlüsseleingaben erfolgen entweder durch Zahlen oder Buchstaben.
Zum Umsetzen der Zahlen in Buchstaben oder umgekehrt dient nachstehende Tafel.
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Enigmail

plugin

mozilla

Thunderbird

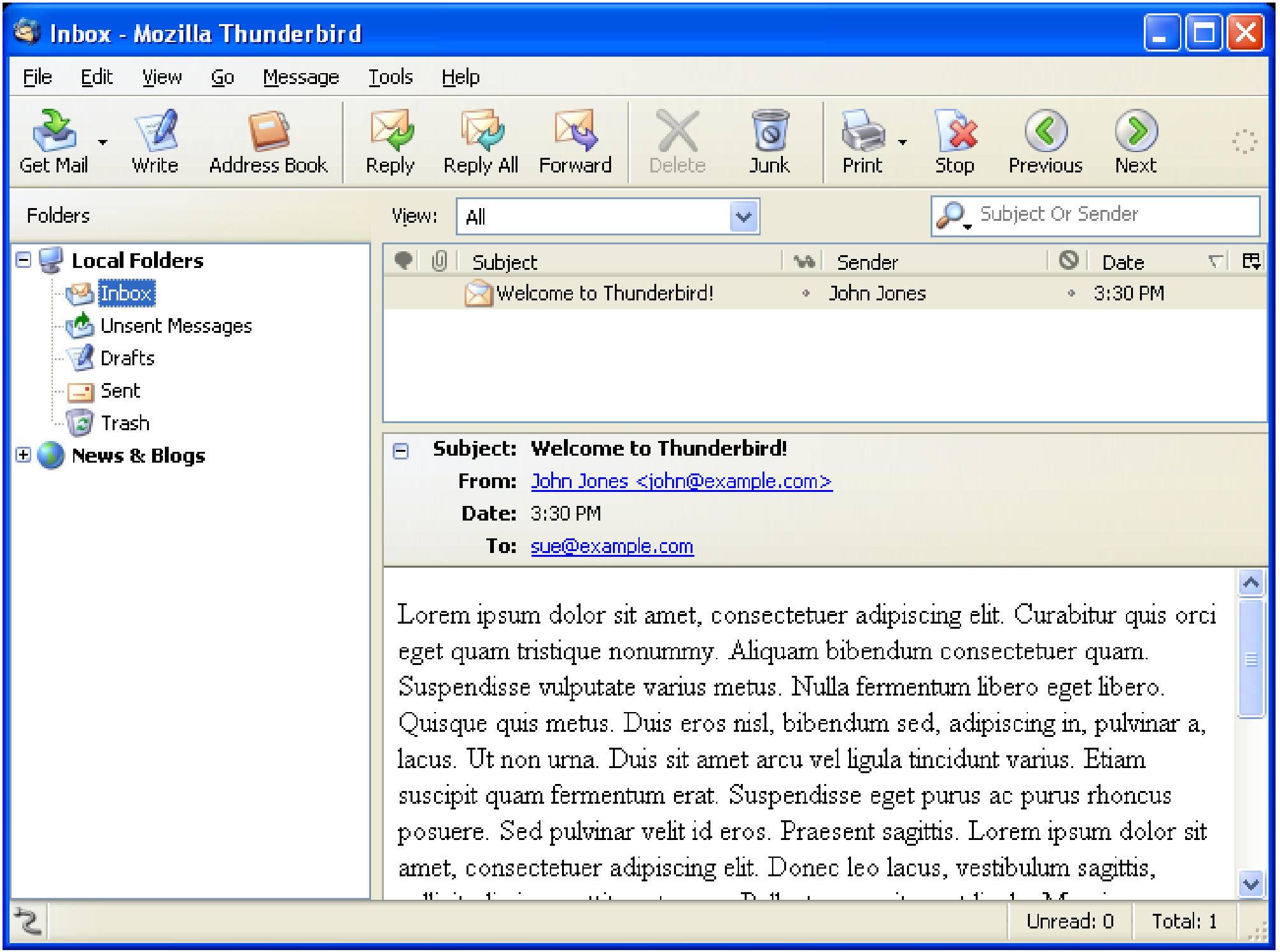
mail reader

mozilla

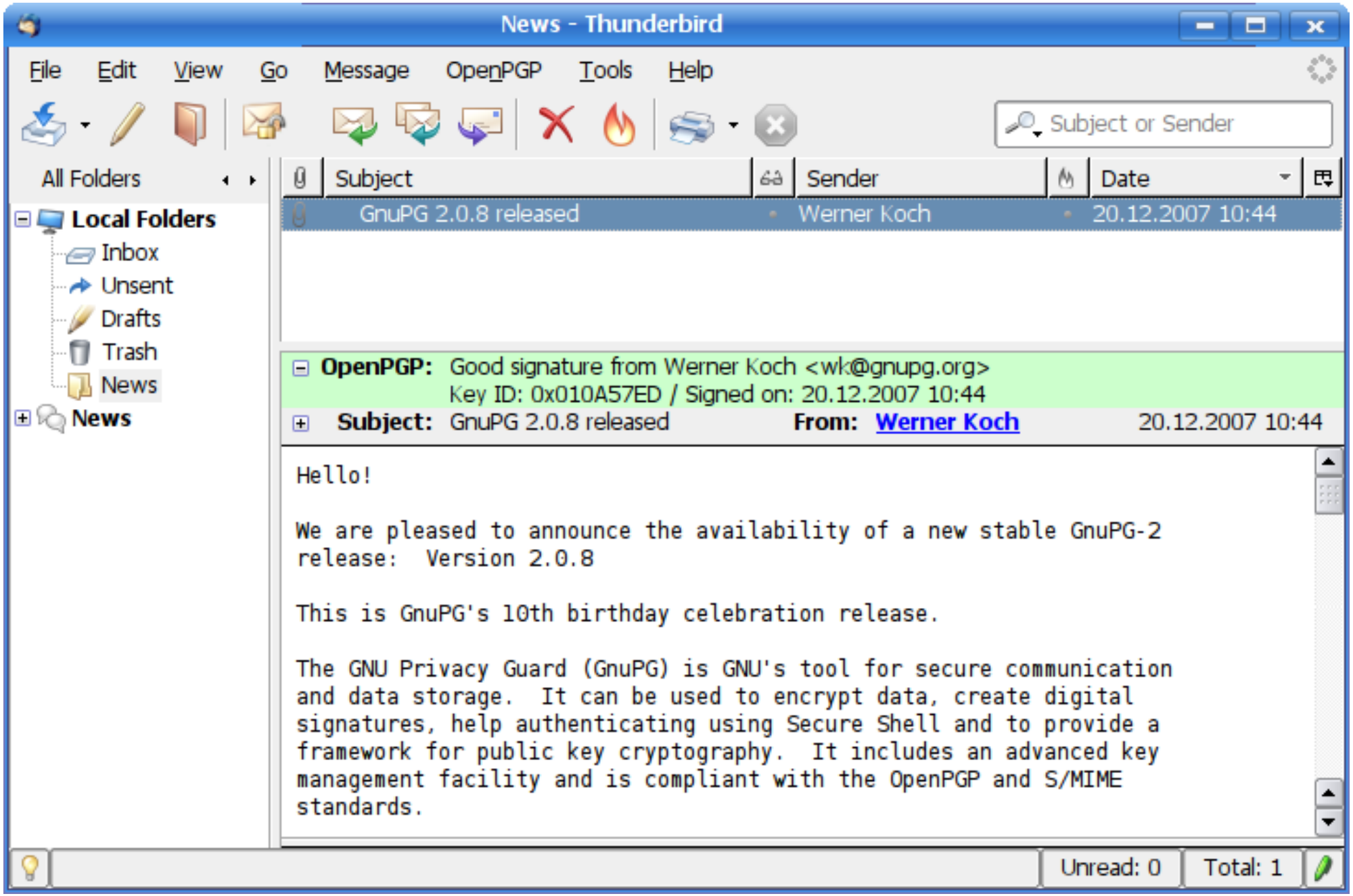
Firefox®

Enigmail

plugin


Inbox - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Delete
Junk
Print
Stop
Previous
Next
Folders
View: All
Subject Or Sender
Local Folders
Inbox
Unsent Messages
Drafts
Sent
Trash
News & Blogs
Subject
Sender
Date
Welcome to Thunderbird!
John Jones
3:30 PM
Subject: Welcome to Thunderbird!
From: John Jones <john@example.com>
Date: 3:30 PM
To: sue@example.com
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Curabitur quis orci eget quam tristique nonummy. Aliquam bibendum consectetuer quam. Suspendisse vulputate varius metus. Nulla fermentum libero eget libero. Quisque quis metus. Duis eros nisl, bibendum sed, adipiscing in, pulvinar a, lacus. Ut non urna. Duis sit amet arcu vel ligula tincidunt varius. Etiam suscipit quam fermentum erat. Suspendisse eget purus ac purus rhoncus posuere. Sed pulvinar velit id eros. Praesent sagittis. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec leo lacus, vestibulum sagittis,
Unread: 0
Total: 1

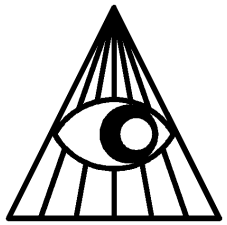
OpenPGP


News - Thunderbird
File Edit View Go Message OpenPGP Tools Help
Subject or Sender
All Folders
Local Folders
Inbox
Unsent
Drafts
Trash
News
News
Subject
Sender
Date
GnuPG 2.0.8 released
Werner Koch
20.12.2007 10:44
OpenPGP: Good signature from Werner Koch <wk@gnupg.org>
Key ID: 0x010A57ED / Signed on: 20.12.2007 10:44
Subject: GnuPG 2.0.8 released
From: Werner Koch
20.12.2007 10:44
Hello!
We are pleased to announce the availability of a new stable GnuPG-2
release: Version 2.0.8
This is GnuPG's 10th birthday celebration release.
The GNU Privacy Guard (GnuPG) is GNU's tool for secure communication
and data storage. It can be used to encrypt data, create digital
signatures, help authenticating using Secure Shell and to provide a
framework for public key cryptography. It includes an advanced key
management facility and is compliant with the OpenPGP and S/MIME
standards.
Unread: 0
Total: 1

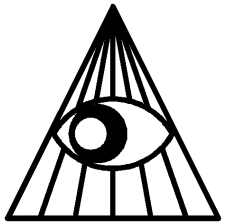
http://enigmail.mozdev.org/

mail

WWW?



HTTP



HTTPS

HTTP*S*

SSL

Secure Socket Layer


Netscape®
™

1994–1996

SSL

SSL 2.0

SSL 3.0

1999

standardized

IETF®

TLS

Transport Layer Security

TLS/SSL

web browser

mozilla
Firefox®

web server

HTTPS

404

Connection refused

problem is on server

HTTPS
not
implemented

HTTPS
not configured

server limits
your security

server
operator?

certificate

certificate
authority

$$

limited choice


Your Certificates
Other People's
Web Sites
Authorities
You have certificates on file that identify these certificate authorities:
Certificate Name
Security Device
GeoTrust Inc.
GlobalSign
GlobalSign nv-sa
Government Root Certification Authority
IPS Internet publishing Services s.l.
IPS Seguridad CA
NetLock Halozatbiztonsagi Kft.
New Dream Network, LLC
QuoVadis Limited
RSA Data Security, Inc.
RSA Security Inc
Root CA
CA Cert Signing Authority
Software Security Device
SECOM Trust.net
Software in the Public Interest, Inc.
Sonera
View
Edit
Import
Delete
OK

pre-loaded

web browser

choice
meaningless


Your Certificates
Other People's
Web Sites
Authorities
You have certificates on file that identify these certificate authorities:
Certificate Name
Security Device
GeoTrust Inc.
GlobalSign
GlobalSign nv-sa
Government Root Certification Authority
IPS Internet publishing Services s.l.
IPS Seguridad CA
NetLock Halozatbiztonsagi Kft.
New Dream Network, LLC
QuoVadis Limited
RSA Data Security, Inc.
RSA Security Inc
Root CA
CA Cert Signing Authority
Software Security Device
SECOM Trust.net
Software in the Public Interest, Inc.
Sonera
View
Edit
Import
Delete
OK

least
trustworthy

make your own

cheap

self-signed certificate

X.509

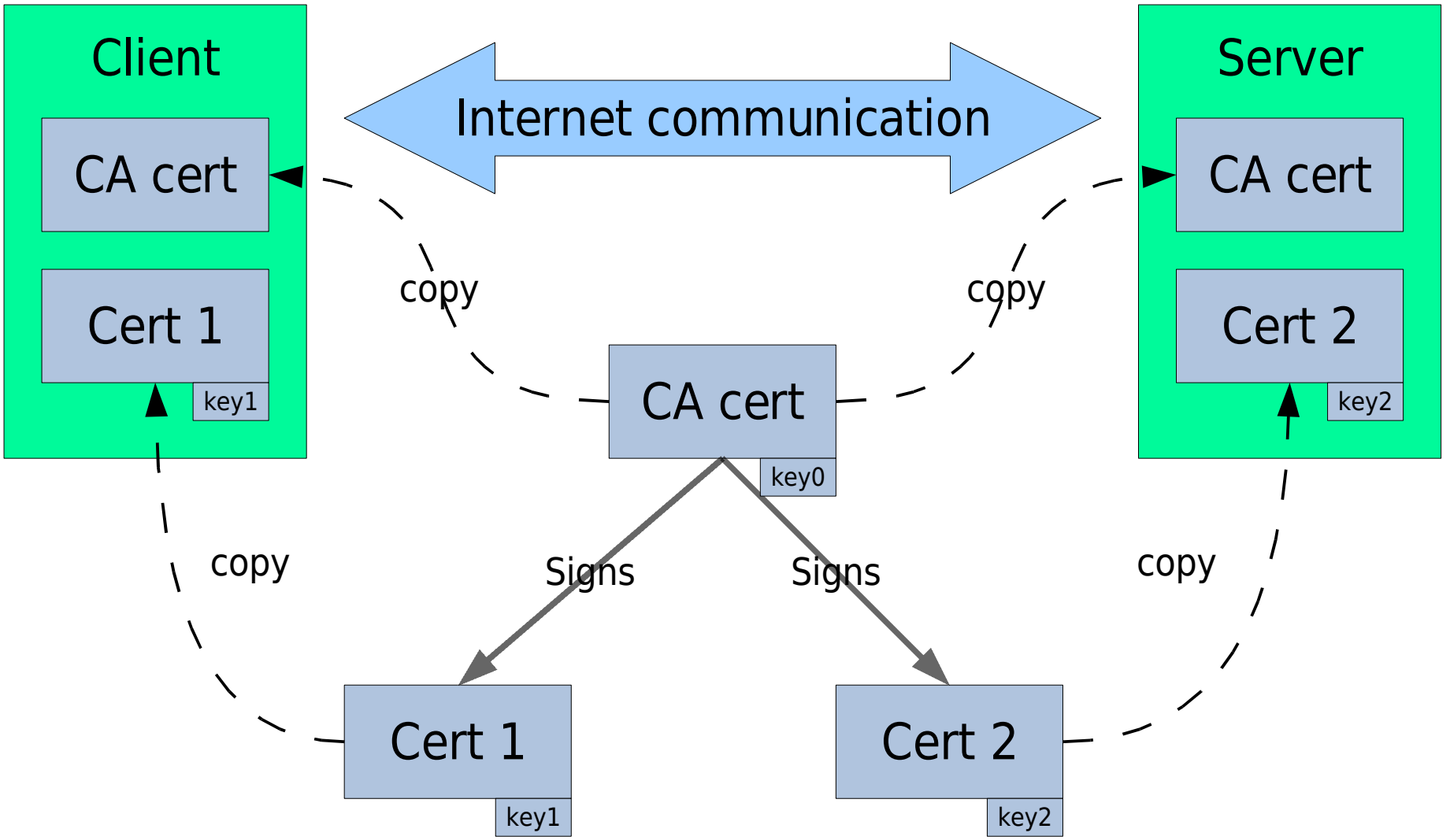
X.509

“Someone tried to explain public-key-based authentication to aliens. Their universal translators were broken and they had to gesture a lot.”
— Peter Gutmann

Everything you Never Wanted to Know about PKI but were Forced to Find Out

X.509 Certificates?

(*very* briefly)



TLS could support OpenPGP keys

not supported
by browsers

not supported by browsers (yet)

self-signed certificate

Unable to verify the identity of cavendish.fsfeurope.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be cavendish.fsfeurope.org, possibly to obtain your confidential information.

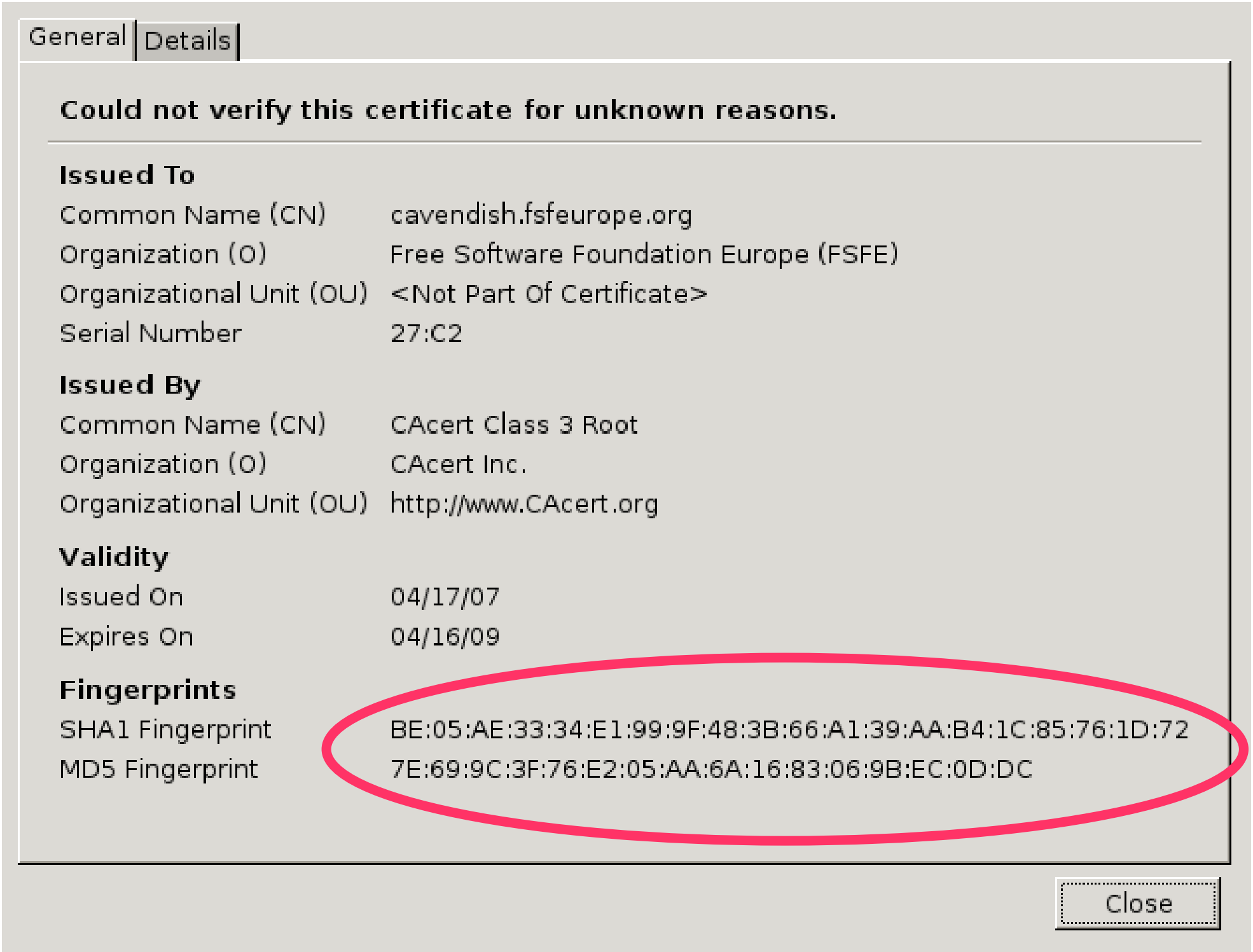
Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site cavendish.fsfeurope.org?

Examine Certificate...

- ○ Accept this certificate permanently
- ◉ Accept this certificate temporarily for this session
- ○ Do not accept this certificate and do not connect to this Web site

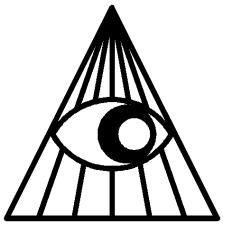
Cancel OK

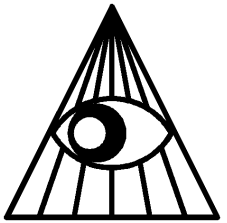

General
Details
Could not verify this certificate for unknown reasons.
Issued To
Common Name (CN) cavendish.fsfeurope.org
Organization (O) Free Software Foundation Europe (FSFE)
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 27:C2
Issued By
Common Name (CN) CAcert Class 3 Root
Organization (O) CAcert Inc.
Organizational Unit (OU) http://www.CAcert.org
Validity
Issued On 04/17/07
Expires On 04/16/09
Fingerprints
SHA1 Fingerprint BE:05:AE:33:34:E1:99:9F:48:3B:66:A1:39:AA:B4:1C:85:76:1D:72
MD5 Fingerprint 7E:69:9C:3F:76:E2:05:AA:6A:16:83:06:9B:EC:0D:DC
Close

web

remote file access

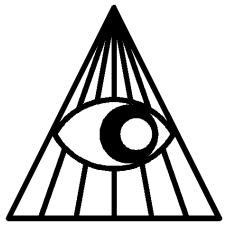
FTP?

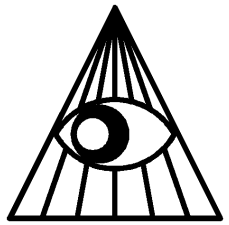




SMB?

(Windows “shared folders”)





(Windows “shared folders”)

FTPS?

(FTP with TLS/SSL)

TLS/SSL

X.509

DO NOT WANT!

SFTP

SSH File Transfer Protocol

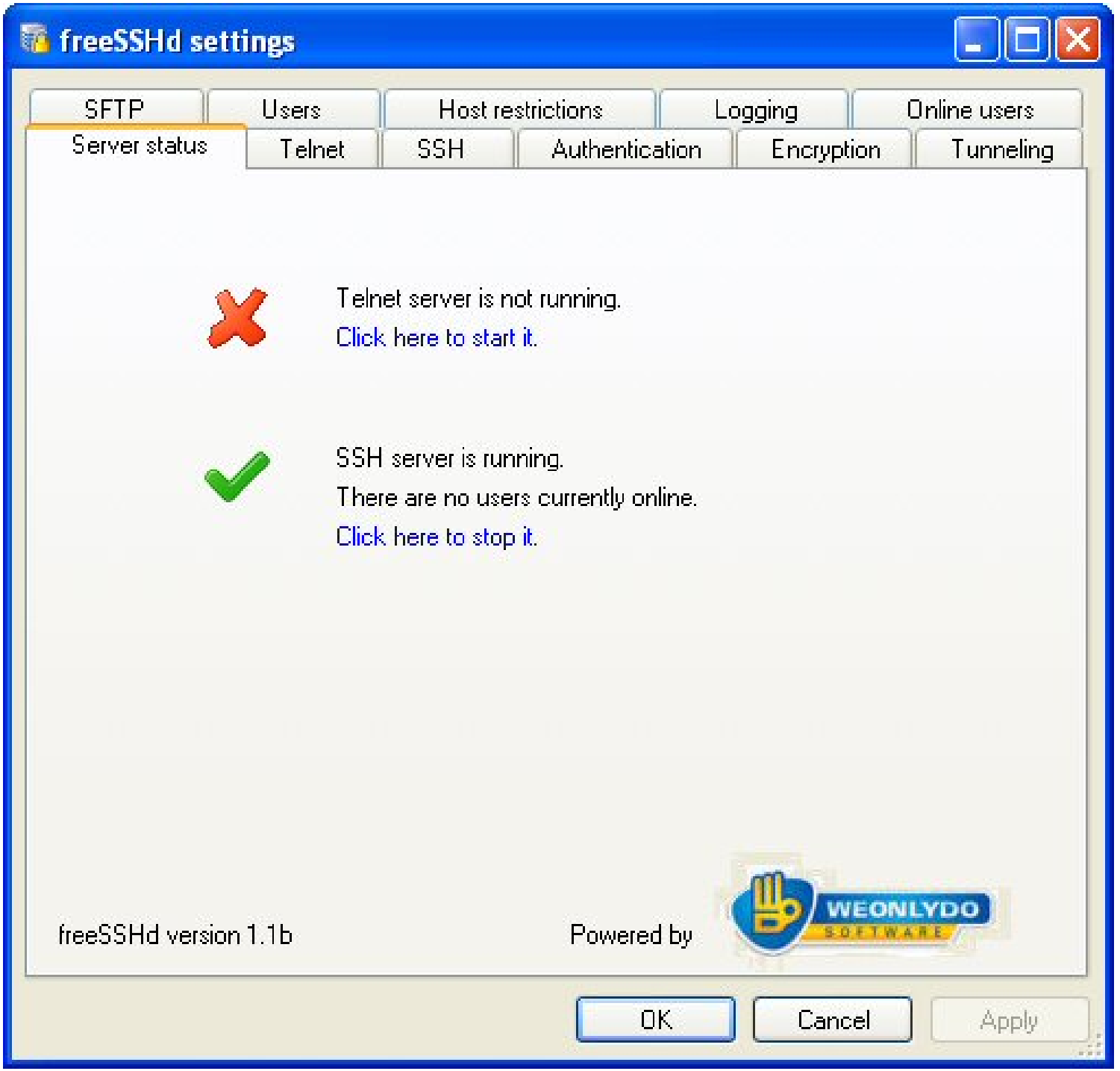
server
Linux/Unix?

easy!
OpenSSH

server
Windows?

FreeSSHd

http://www.freesshd.com/


freeSSHd settings
SFTP
Users
Host restrictions
Logging
Online users
Server status
Telnet
SSH
Authentication
Encryption
Tunneling
Telnet server is not running.
Click here to start it.
SSH server is running.
There are no users currently online.
Click here to stop it.
freeSSHd version 1.1b
Powered by
WEONLYDO
SOFTWARE
OK
Cancel
Apply

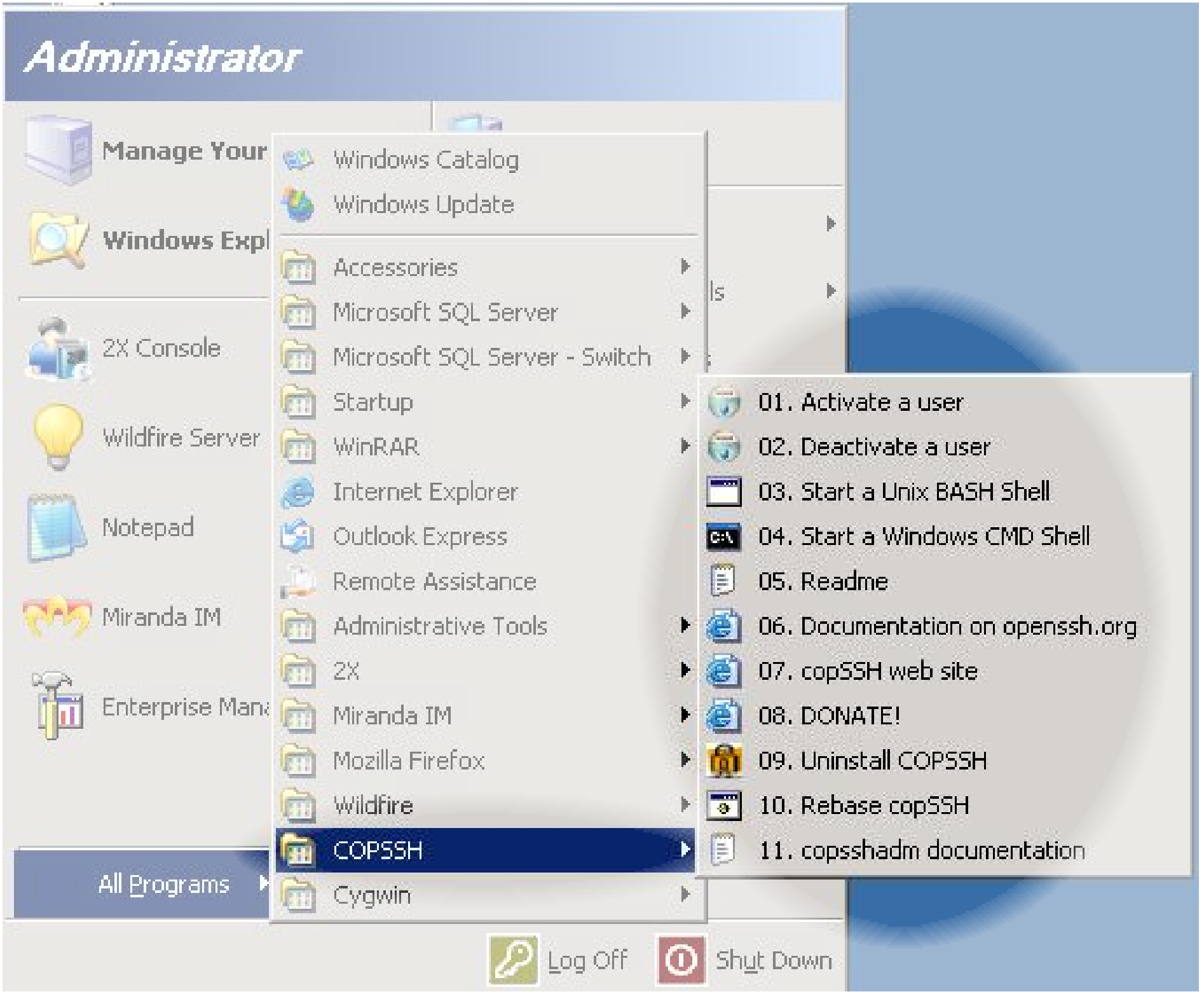
(freeware,
not open source)

Free Software

copSSH

http://www.itefix.no/

OpenSSH


Administrator
Manage Your
Windows Expl
2X Console
Wildfire Server
Notepad
Miranda IM
Enterprise Mana
All Programs
Windows Catalog
Windows Update
Accessories
Microsoft SQL Server
Microsoft SQL Server - Switch
Startup
WinRAR
Internet Explorer
Outlook Express
Remote Assistance
Administrative Tools
2X
Miranda IM
Mozilla Firefox
Wildfire
COPSSH
Cygwin
01. Activate a user
02. Deactivate a user
03. Start a Unix BASH Shell
04. Start a Windows CMD Shell
05. Readme
06. Documentation on openssh.org
07. copSSH web site
08. DONATE!
09. Uninstall COPSSH
10. Rebase copSSH
11. copsshadm documentation
Log Off
Shut Down

OpenSSH by hand

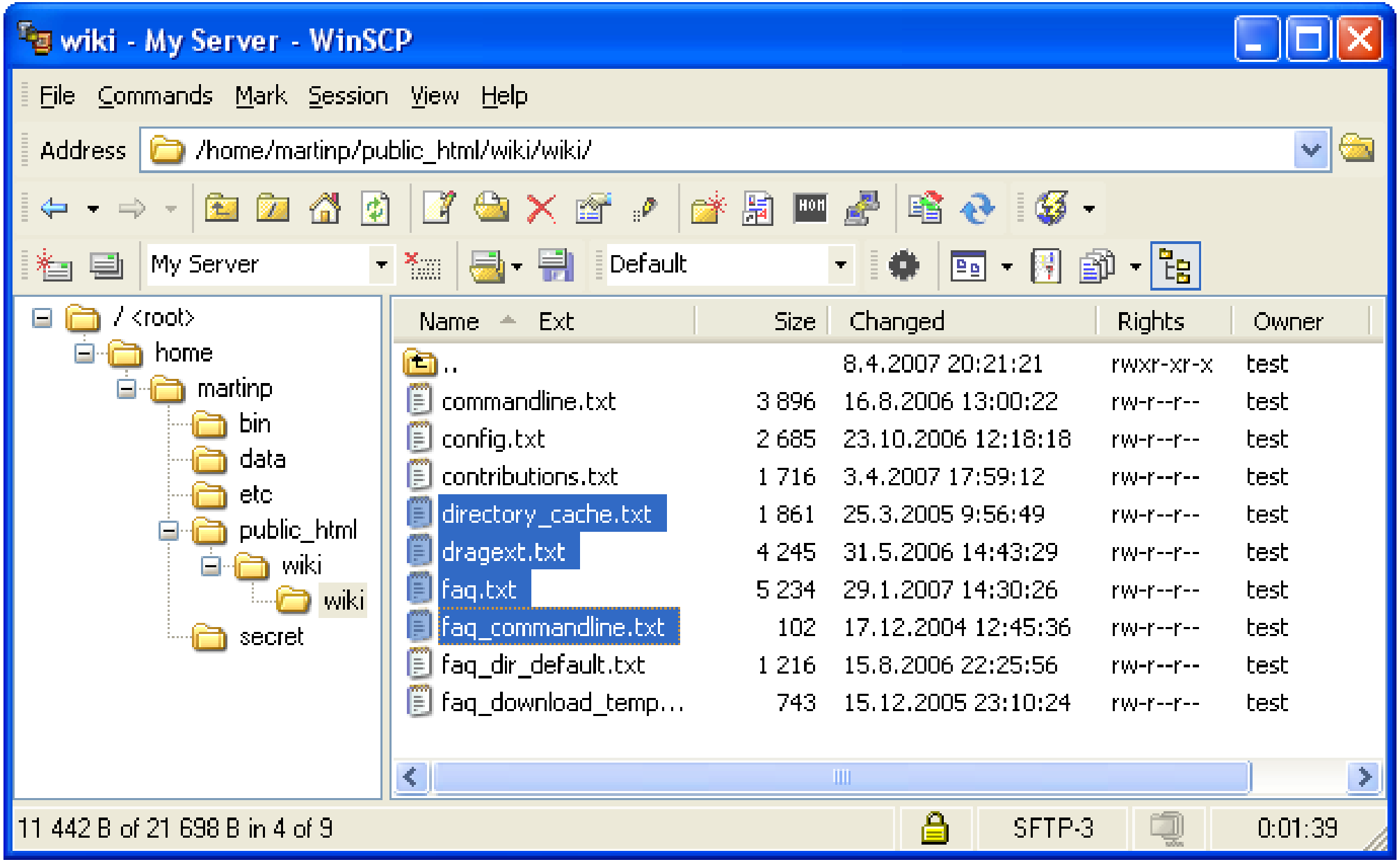
OpenSSH for Windows

http://pigtail.net/LRP/printsrv/cygwin-sshd.html

server

client?

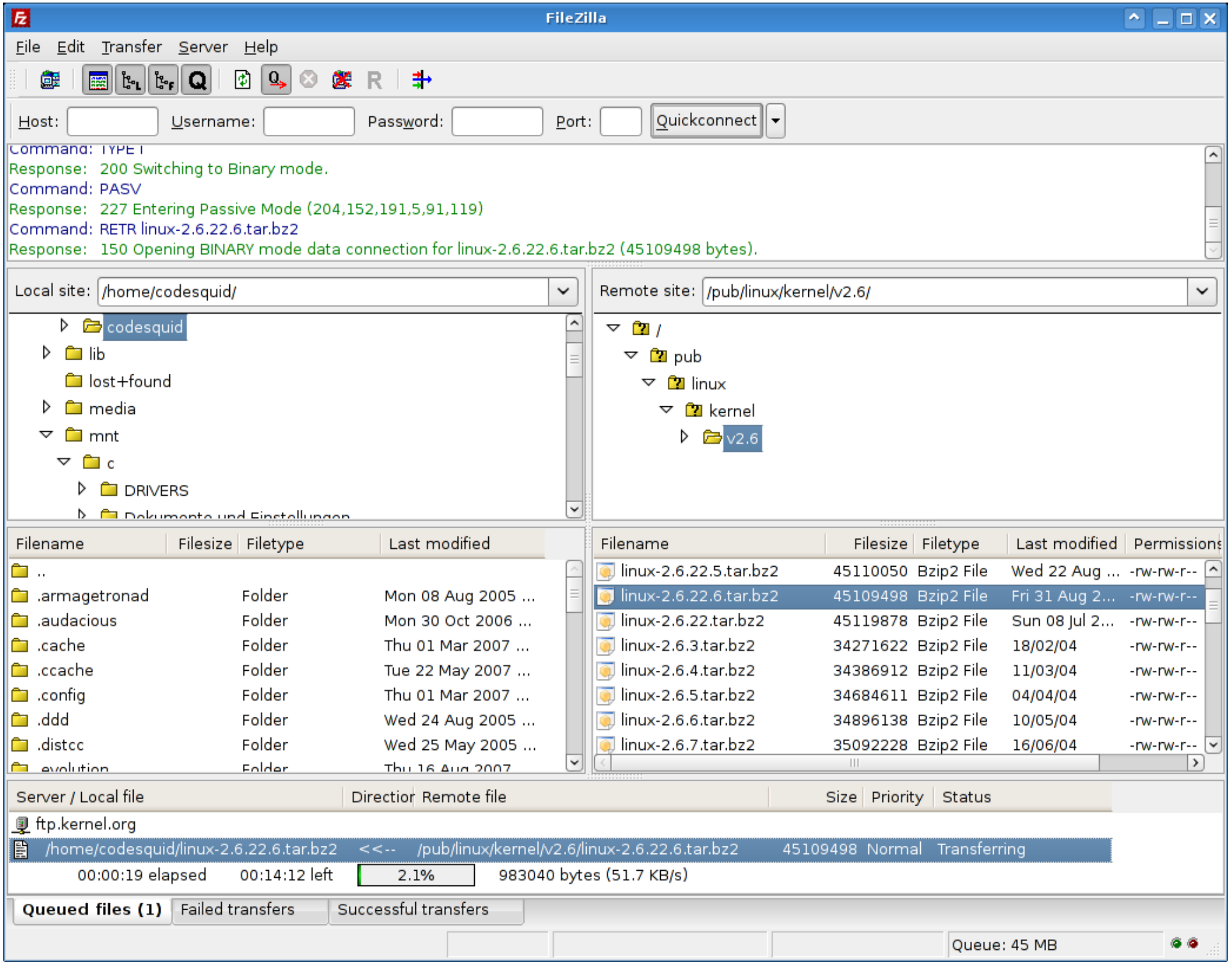
WinSCP


wiki - My Server - WinSCP
File Commands Mark Session View Help
Address /home/martinp/public_html/wiki/wiki/
My Server
Default
/ <root>
home
martinp
bin
data
etc
public_html
wiki
wiki
secret
Name Ext Size Changed Rights Owner
.. 8.4.2007 20:21:21 rwxr-xr-x test
commandline.txt 3 896 16.8.2006 13:00:22 rw-r--r-- test
config.txt 2 685 23.10.2006 12:18:18 rw-r--r-- test
contributions.txt 1 716 3.4.2007 17:59:12 rw-r--r-- test
directory_cache.txt 1 861 25.3.2005 9:56:49 rw-r--r-- test
dragext.txt 4 245 31.5.2006 14:43:29 rw-r--r-- test
faq.txt 5 234 29.1.2007 14:30:26 rw-r--r-- test
faq_commandline.txt 102 17.12.2004 12:45:36 rw-r--r-- test
faq_dir_default.txt 1 216 15.8.2006 22:25:56 rw-r--r-- test
faq_download_temp... 743 15.12.2005 23:10:24 rw-r--r-- test
11 442 B of 21 698 B in 4 of 9
SFTP-3
0:01:39

Windows only

FileZilla

Windows & Linux


FileZilla
File Edit Transfer Server Help
Host: Username: Password: Port: Quickconnect
Command: TYPE I
Response: 200 Switching to Binary mode.
Command: PASV
Response: 227 Entering Passive Mode (204,152,191,5,91,119)
Command: RETR linux-2.6.22.6.tar.bz2
Response: 150 Opening BINARY mode data connection for linux-2.6.22.6.tar.bz2 (45109498 bytes).
Local site: /home/codesquid/
codesquid
lib
lost+found
media
mnt
c
DRIVERS
Remote site: /pub/linux/kernel/v2.6/
/
pub
linux
kernel
v2.6
Filename Filesize Filetype Last modified
.. Folder
.armagetronad Folder Mon 08 Aug 2005 ...
.audacious Folder Mon 30 Oct 2006 ...
.cache Folder Thu 01 Mar 2007 ...
.ccache Folder Tue 22 May 2007 ...
.config Folder Thu 01 Mar 2007 ...
.ddd Folder Wed 24 Aug 2005 ...
.distcc Folder Wed 25 May 2005 ...
Filename Filesize Filetype Last modified Permissions
linux-2.6.22.5.tar.bz2 45110050 Bzip2 File Wed 22 Aug ... -rw-rw-r--
linux-2.6.22.6.tar.bz2 45109498 Bzip2 File Fri 31 Aug 2... -rw-rw-r--
linux-2.6.22.tar.bz2 45119878 Bzip2 File Sun 08 Jul 2... -rw-rw-r--
linux-2.6.3.tar.bz2 34271622 Bzip2 File 18/02/04 -rw-rw-r--
linux-2.6.4.tar.bz2 34386912 Bzip2 File 11/03/04 -rw-rw-r--
linux-2.6.5.tar.bz2 34684611 Bzip2 File 04/04/04 -rw-rw-r--
linux-2.6.6.tar.bz2 34896138 Bzip2 File 10/05/04 -rw-rw-r--
linux-2.6.7.tar.bz2 35092228 Bzip2 File 16/06/04 -rw-rw-r--
Server / Local file Direction Remote file Size Priority Status
ftp.kernel.org
/home/codesquid/linux-2.6.22.6.tar.bz2 <<-- /pub/linux/kernel/v2.6/linux-2.6.22.6.tar.bz2 45109498 Normal Transferring
00:00:19 elapsed 00:14:12 left 2.1% 983040 bytes (51.7 KB/s)
Queued files (1) Failed transfers Successful transfers
Queue: 45 MB

remote file access

remote desktop

none are
Free Software

Linux/Unix

X11 through SSH tunnel

SSH server

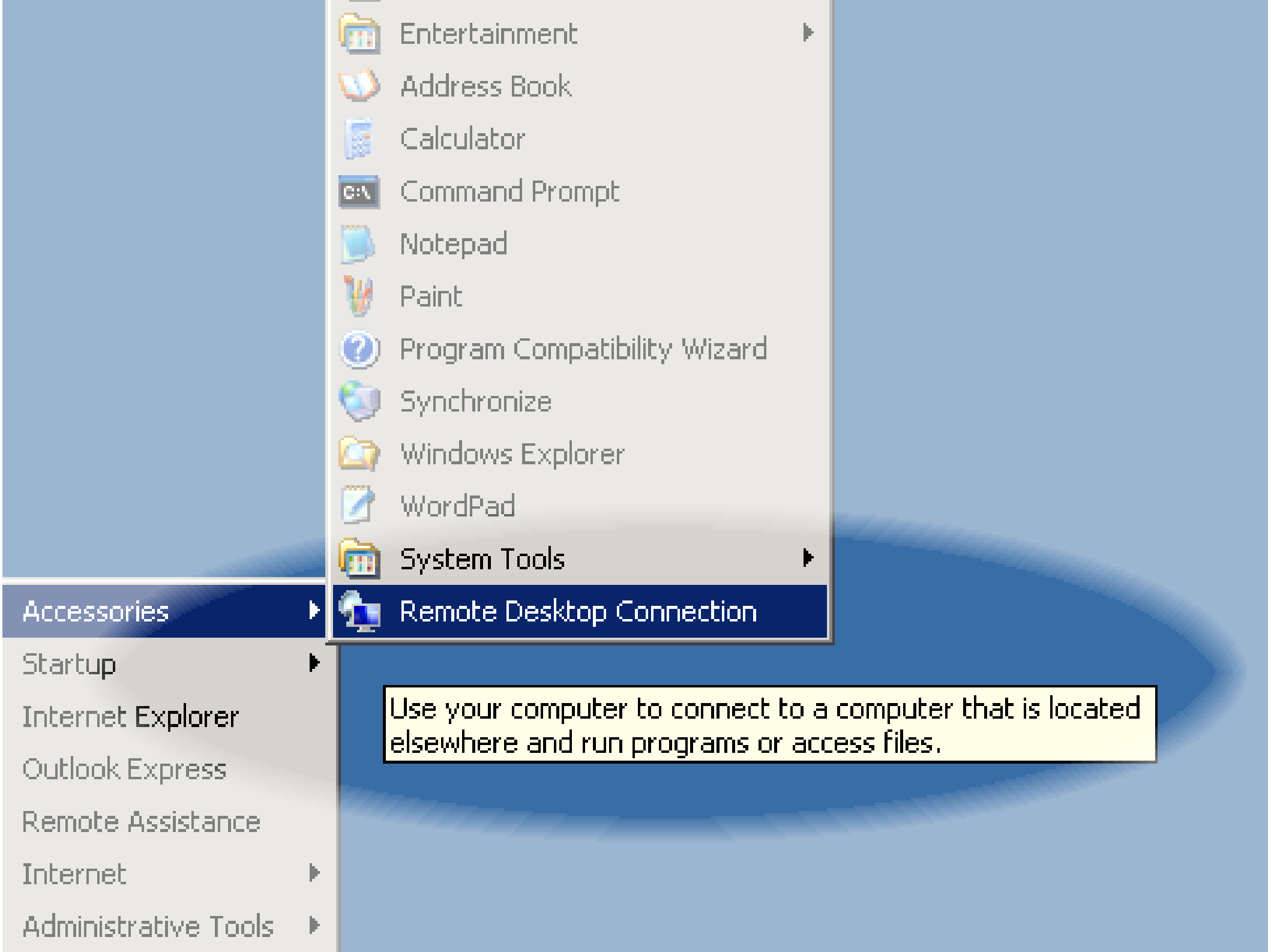
SSH tunnel

tunnel RDP

tunnel VNC

RDP

Windows “Remote Desktop Protocol”


Entertainment
Address Book
Calculator
Command Prompt
Notepad
Paint
Program Compatibility Wizard
Synchronize
Windows Explorer
WordPad
System Tools
Accessories
Remote Desktop Connection
Startup
Internet Explorer
Outlook Express
Remote Assistance
Internet
Administrative Tools
Use your computer to connect to a computer that is located elsewhere and run programs or access files.

VNC

Virtual Network Computing

TightVNC

http://www.tightvnc.com/

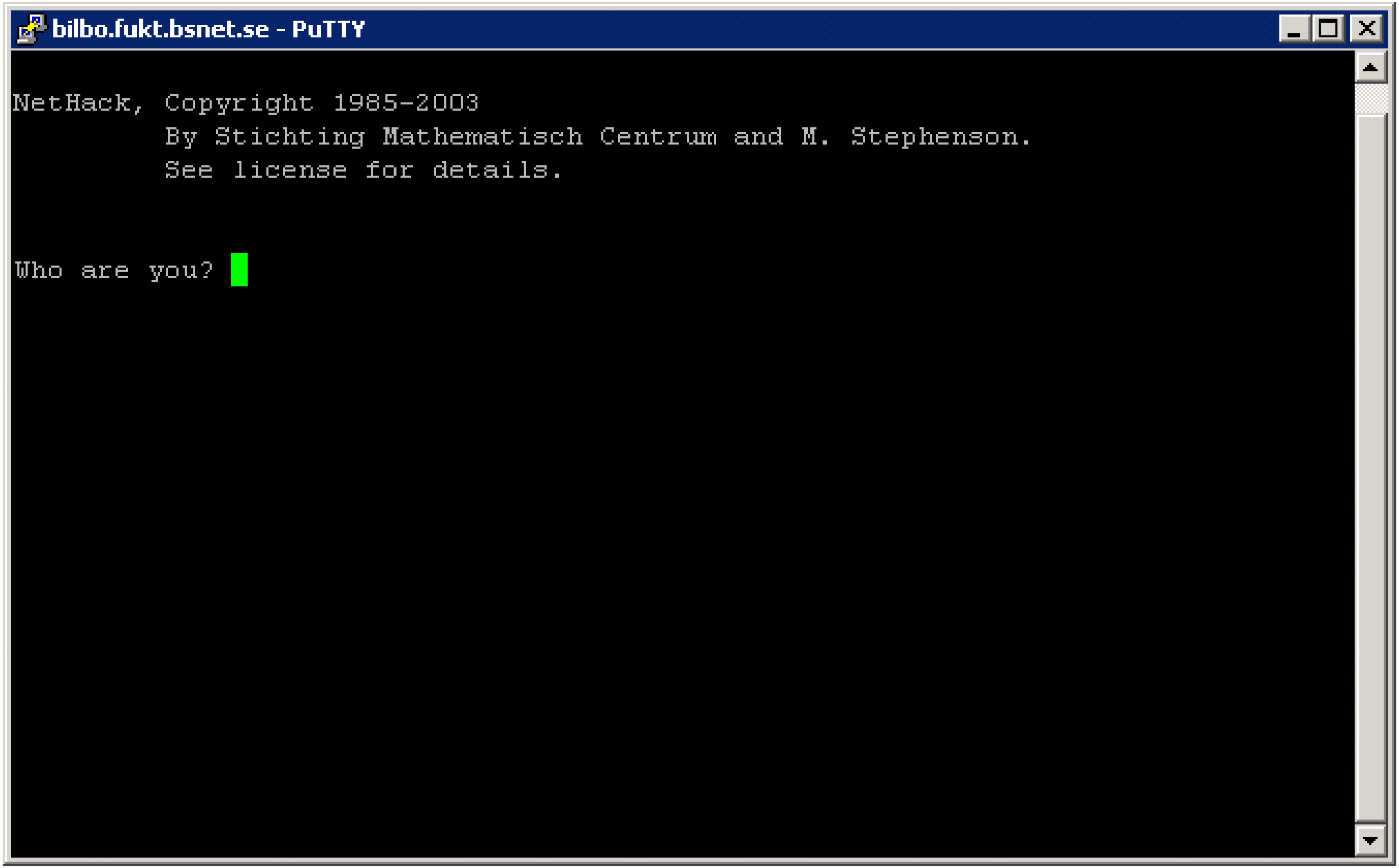
remote desktop

remote
terminal

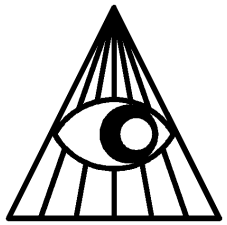
SSH

Windows

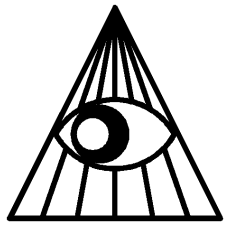
PuTTY


bilbo.fukt.bsnet.se - PuTTY
NetHack, Copyright 1985-2003
By Stichting Mathematisch Centrum and M. Stephenson.
See license for details.
Who are you?

p2p
file sharing



BitTorrent



Azureus

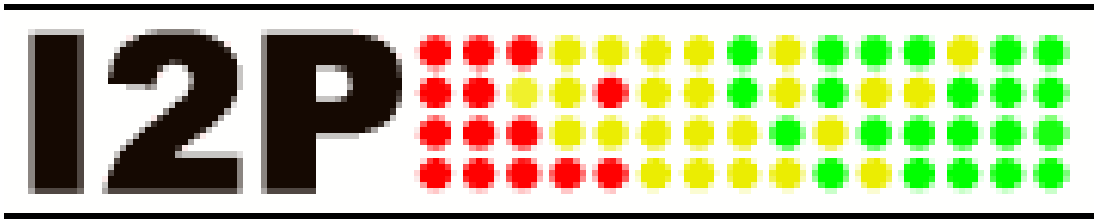
Perfect Dark

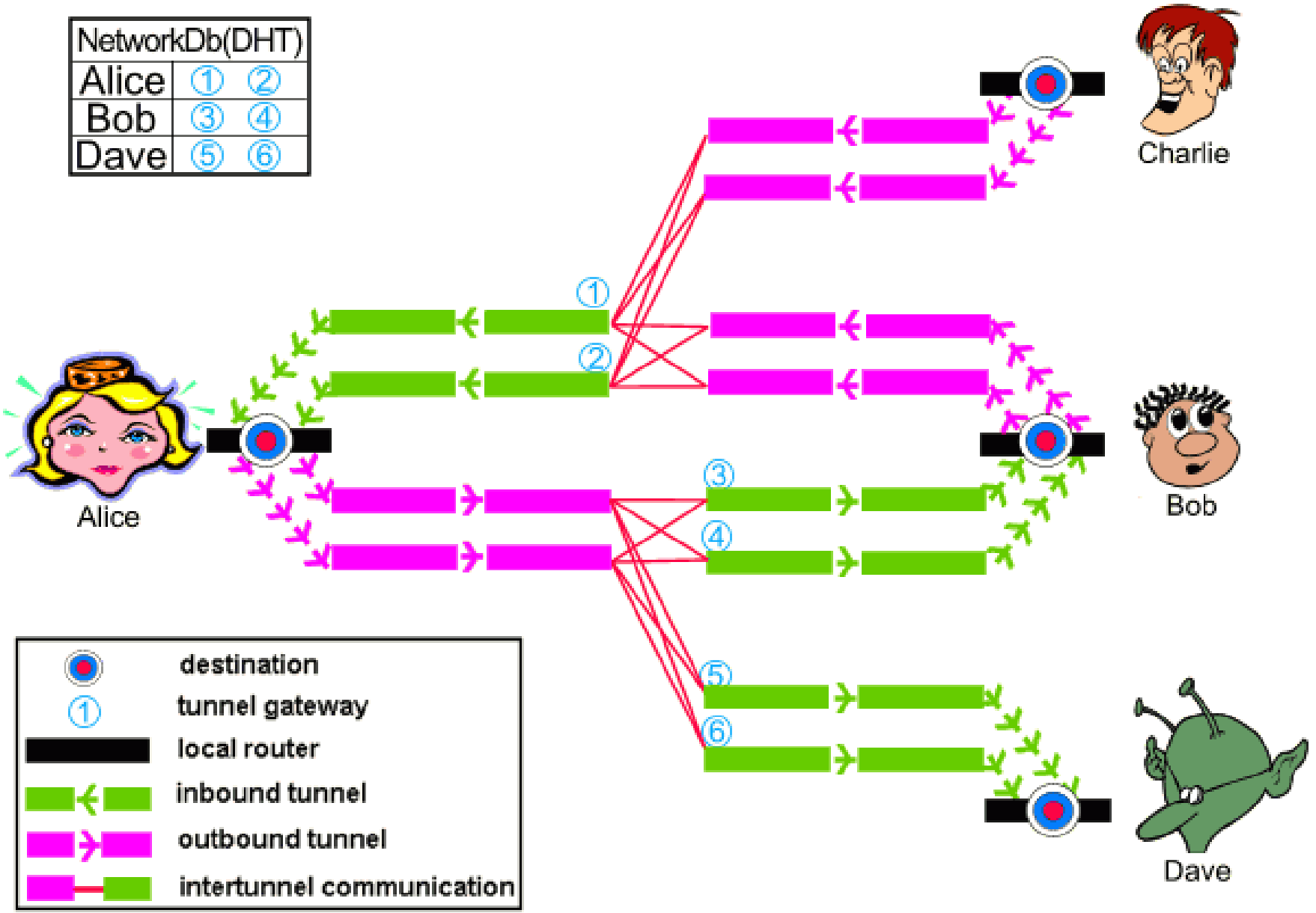
日本語！

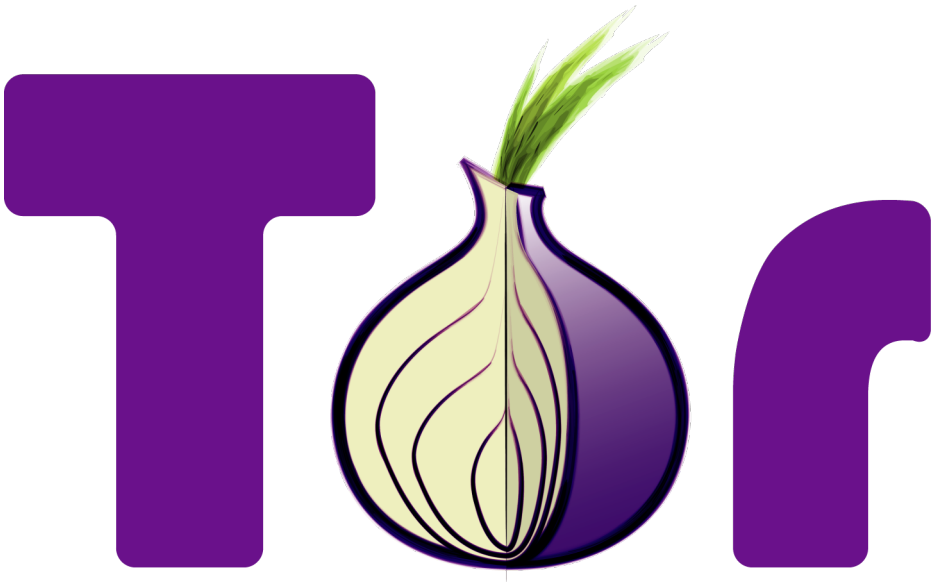
ANts

GNUnet

RShare


I2P


NetworkDb(DHT)
Alice ① ②
Bob ③ ④
Dave ⑤ ⑥
Charlie
Alice
Bob
Dave
destination
tunnel gateway
local router
inbound tunnel
outbound tunnel
intertunnel communication


Tor

p2p
file sharing

VPN tunnels

must be set up
in advance

both sides

IPsec

structurally
cleaner

very complex

(see separate Ipsec lecture)

OpenVPN

non-standard protocol

should be avoided

security concerns

standards
interoperability

however

easy to set up

endorsed by experts

standards
interoperability

OpenVPN

network

stolen laptop

whole-disk encryption

TrueCrypt

TrueCrypt Volume Creation Wizard

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, 14 rounds, 128-bit block (AES-256, published in 2001). Mode of operation is LRW.

Benchmark

Hash Algorithm

Whirlpool

Help | < Prev | Next > | Cancel

non-standard

not in kernel

no other implementation

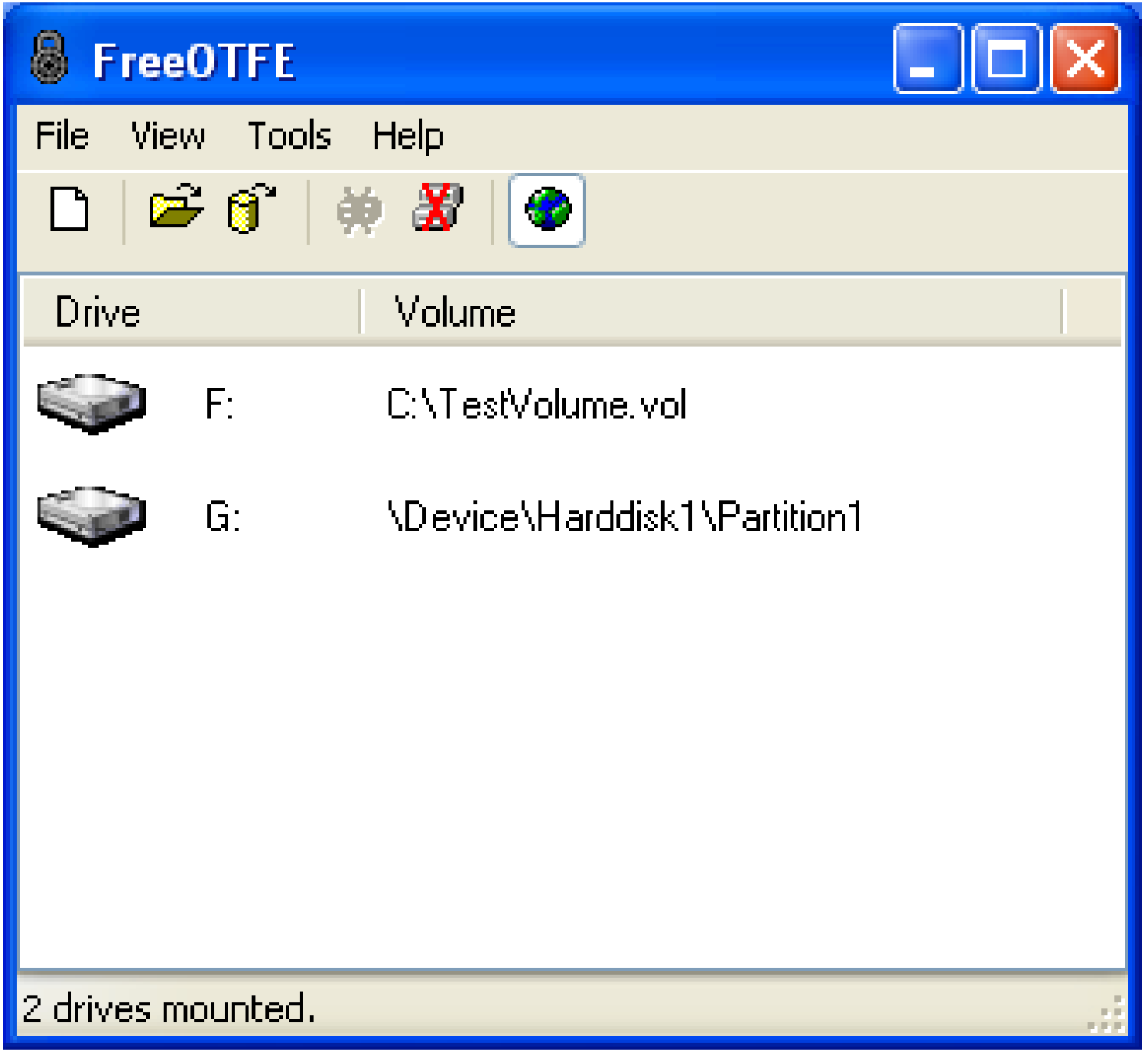
dual-platform

dm-crypt/LUKS

in kernel

FreeOTFE

http://www.freeotfe.org/


FreeOTFE
File
View
Tools
Help
Drive
Volume
F:
C:\TestVolume.vol
G:
\Device\Harddisk1\Partition1
2 drives mounted.

can read dm-crypt/LUKS

FAT/NTFS

boot-time whole-disk encryption

dm-crypt/LUKS

/boot
unencrypted

/boot on USB key

small gain

unfeasible for servers

password?

password in /boot file

vulnerable to computer seizure

password on USB key

enter password
at boot

neither
works for
server hosts

need
unattended
reboots

Mandos

gives
passwords to
hosts

uses TLS

all hosts run Mandos queryer

host key stored in /boot

one host runs Mandos responder

host down
too long?

host gets no password

unattended reboots

security from server seizure

some security