# Cryptography: Practice

2013 JMU Cyber Defense Boot Camp

# Prerequisites

- This unit assumes that you have already known
  - Symmetric-key encryption
  - Public-key encryption
  - Digital signature
  - Digital certificates

# Step 0

- Use Firefox to log into your vCenter server and find your Windows 2003 VM
- Use the “**WLAN and Crypto Security**” VM snapshot

# Organization

- Practice
  - Truecrypt
  - GPG

# Road Map

- Practice
  - Truecrypt
  - GPG

# TrueCrypt

- Open-source disk encryption software
  - Not just encrypting single files, but the whole disk
- Supports Windows, Linux, and Mac OS
  - [http://www.truecrypt.org/](http://www.truecrypt.org/)
- Has been used by "bad people" to encrypt laptops and external hard disks

# Step 1

- Download and install
  - http://www.truecrypt.org/downloads

- **NOTE:** TrueCrypt has already been installed on your Windows 2003 VM under the "**WLAN and Crypto Security**" VM snapshot

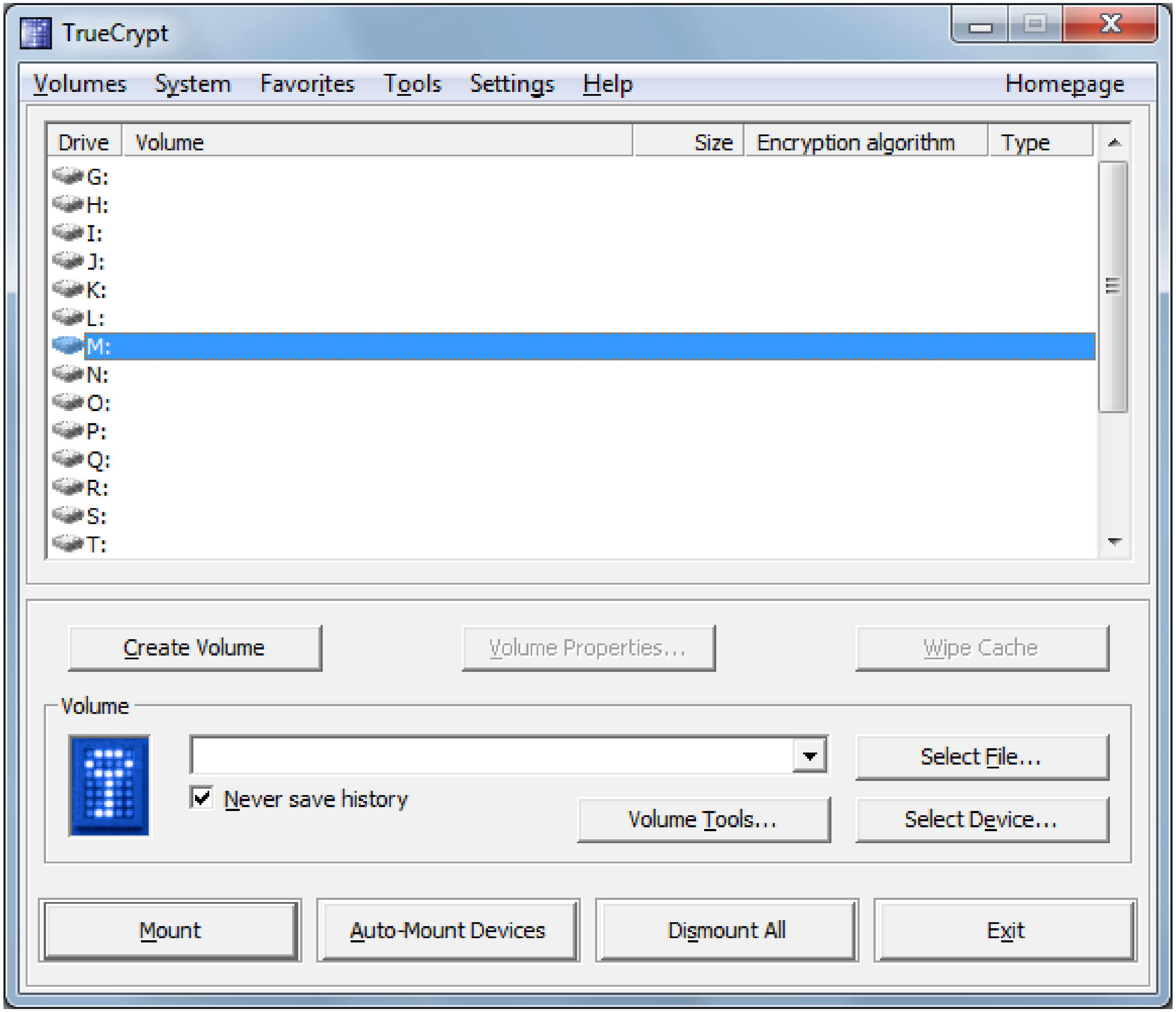
# Step 2: Run TrueCrypt

- Start > All Programs > TrueCrypt > TrueCrypt

- (You can also run it directly from a shortcut on your Desktop)

# Step 2

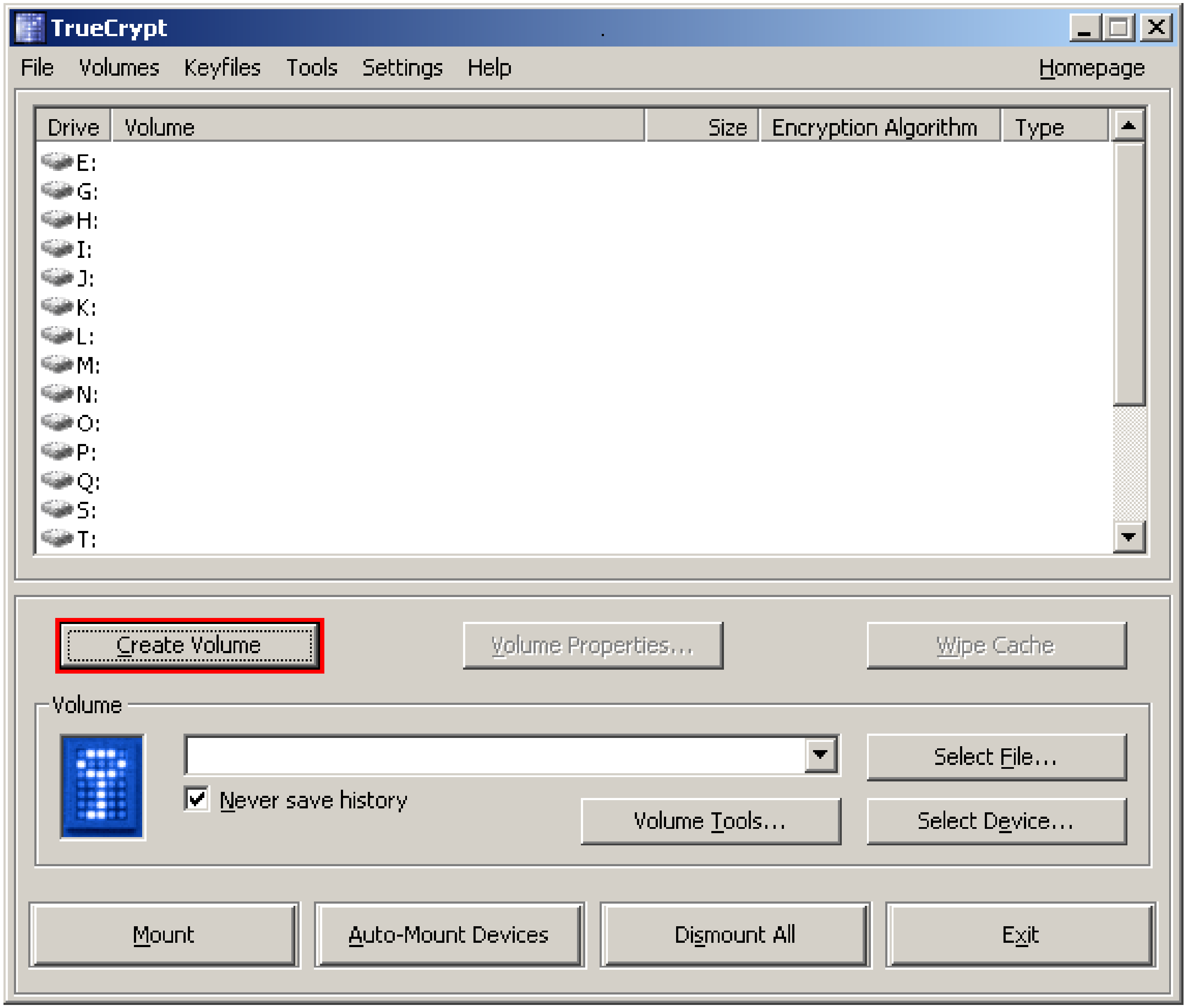
- Create a virtual encrypted disk (called file containers)
  - Put all of your critical files there

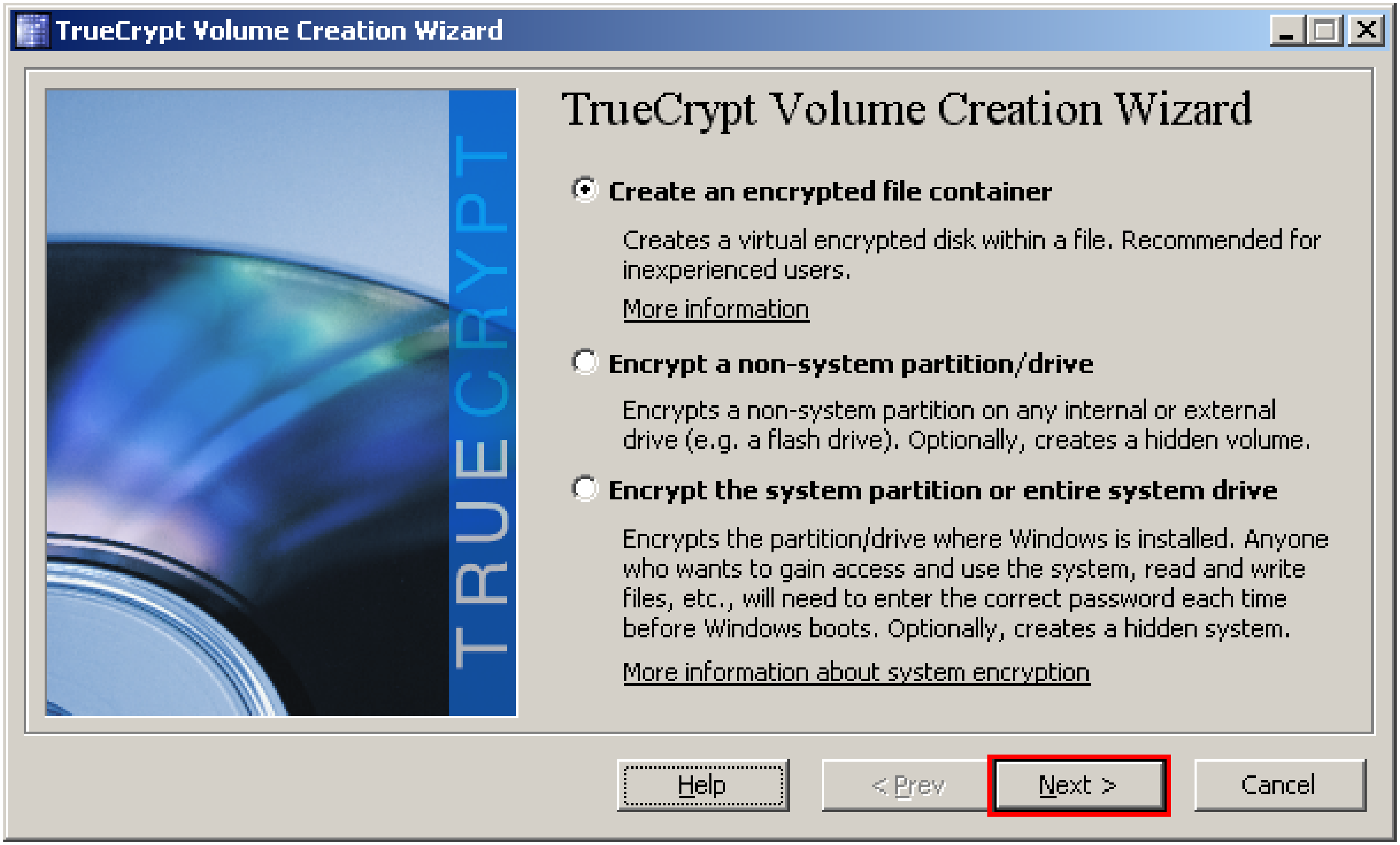


| Drive | Volume | Size | Encryption algorithm | Type |
|---|---|---|---|---|
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | | | | |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| R: | | | | |
| S: | | | | |
| T: | | | | |

☑ Never save history

**CREDITS**: some of these screen snapshots are from http://www.truecrypt.org/docs/





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**

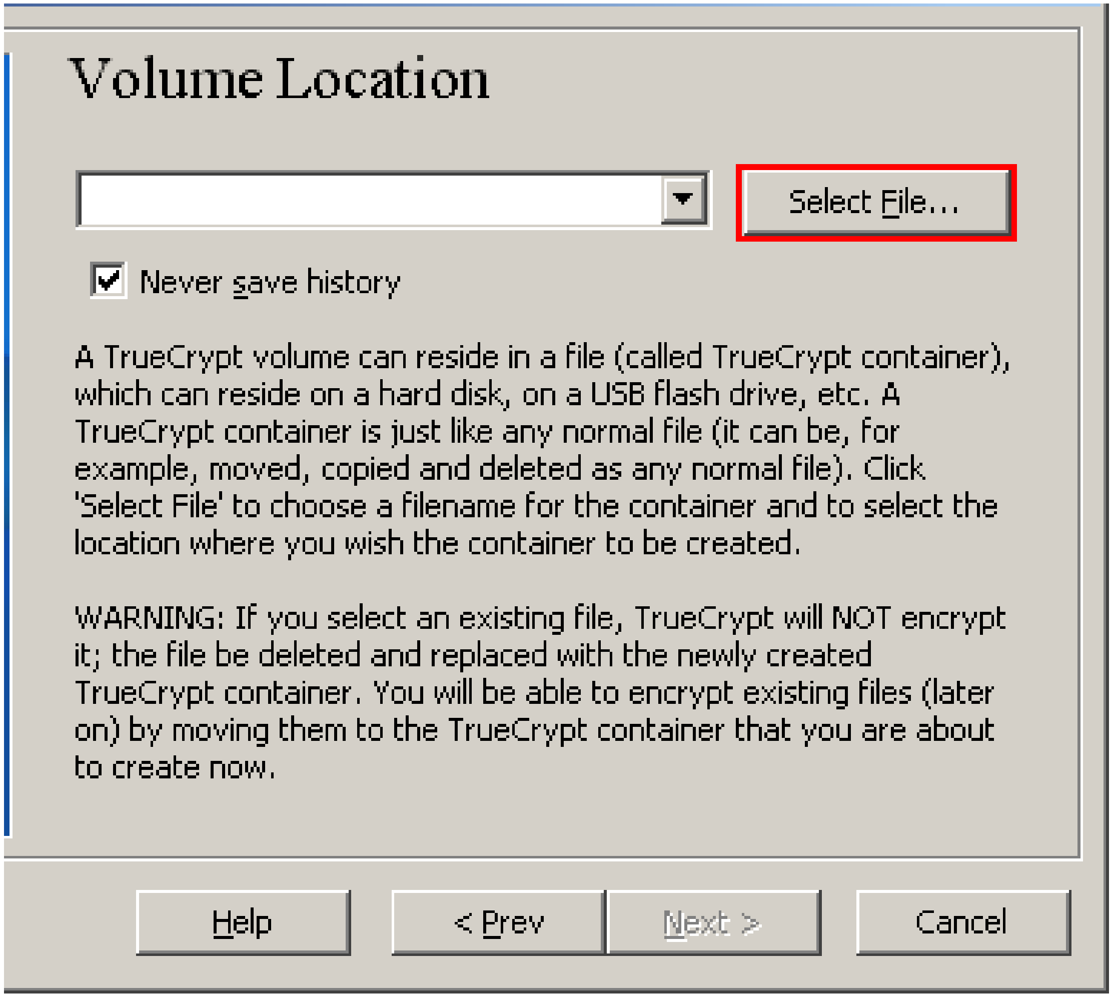
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **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

# The Location of the Virtual Encrypted Disk

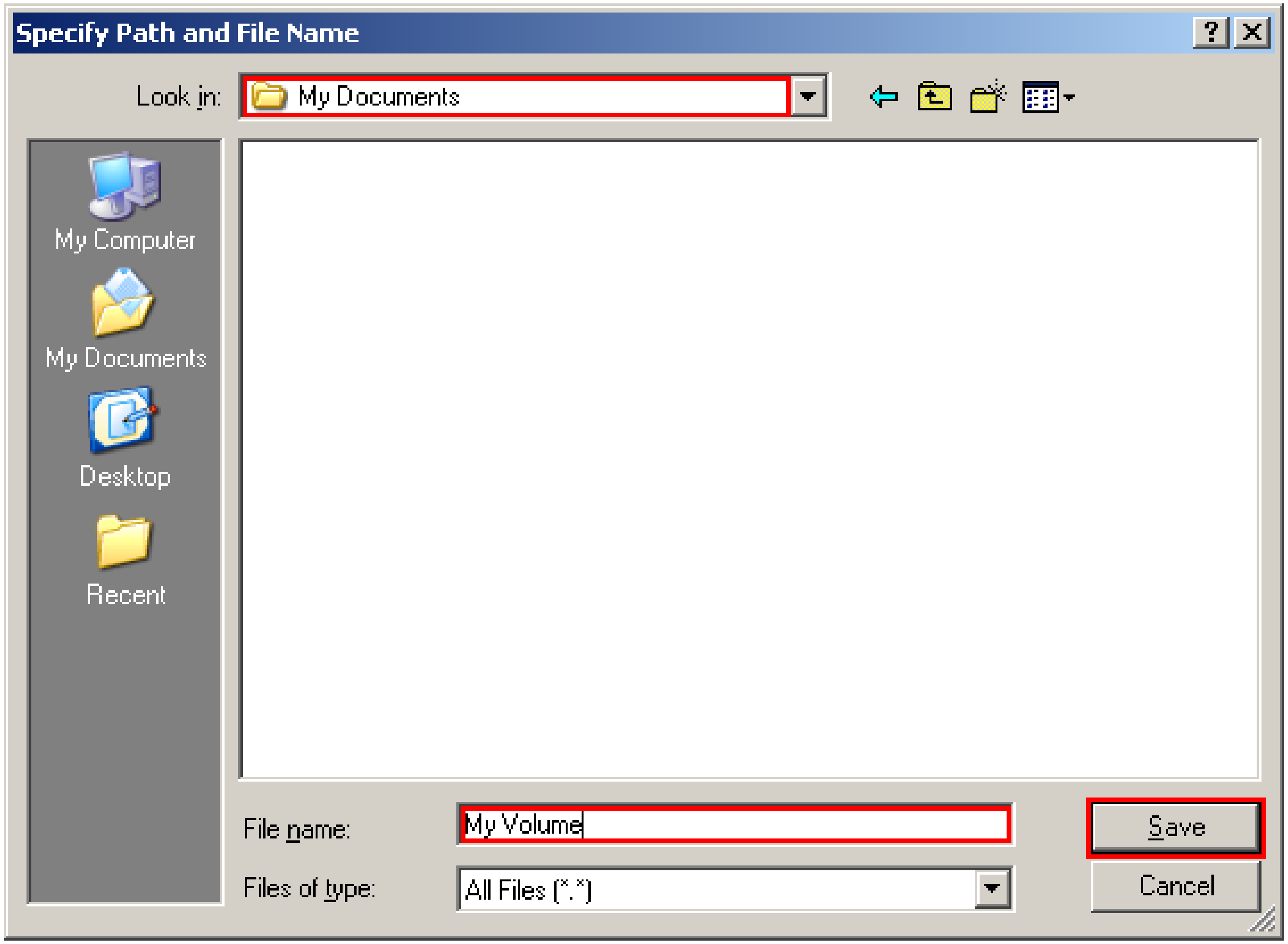


Volume Location

☑ 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, copied and 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 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.

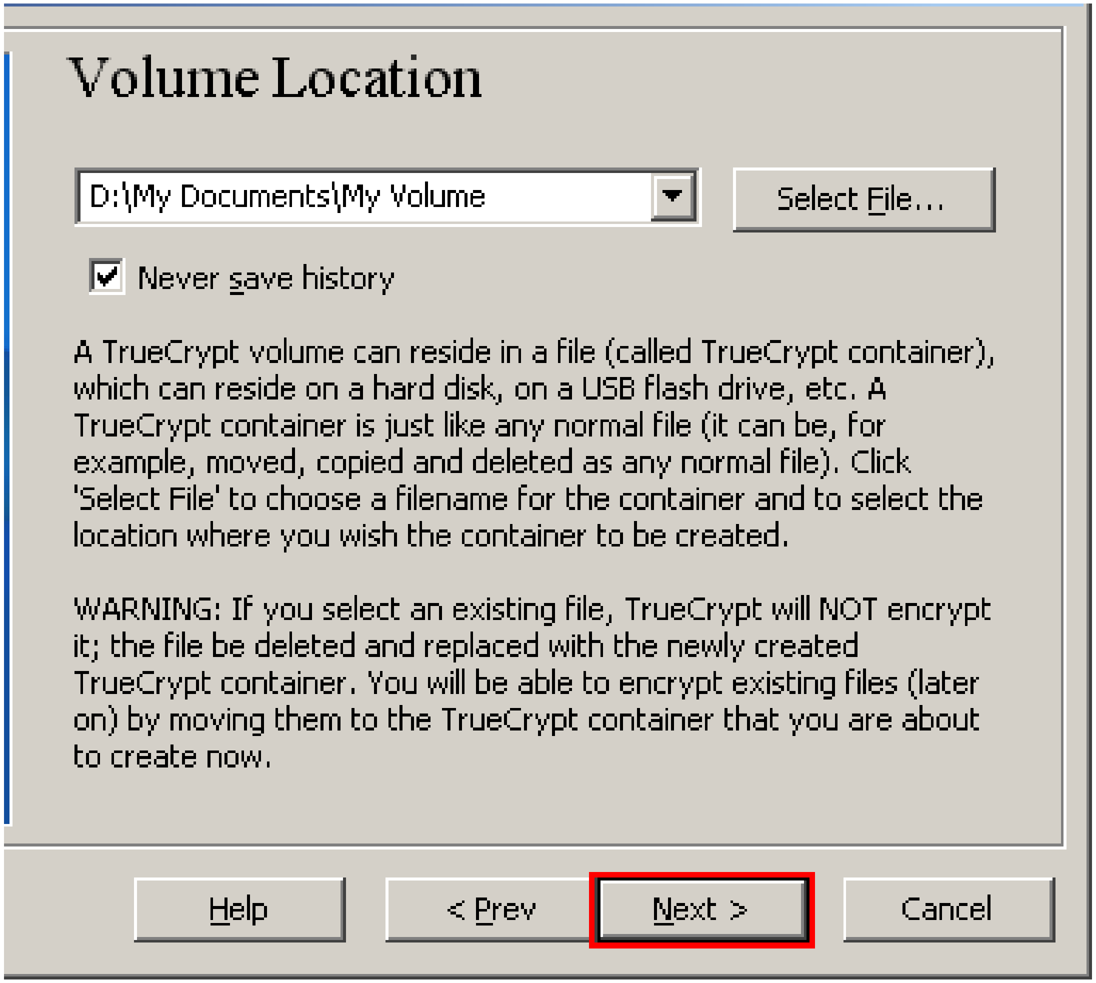


Specify Path and File Name

Look in: My Documents

File name: My Volume

Files of type: All Files (*.*)



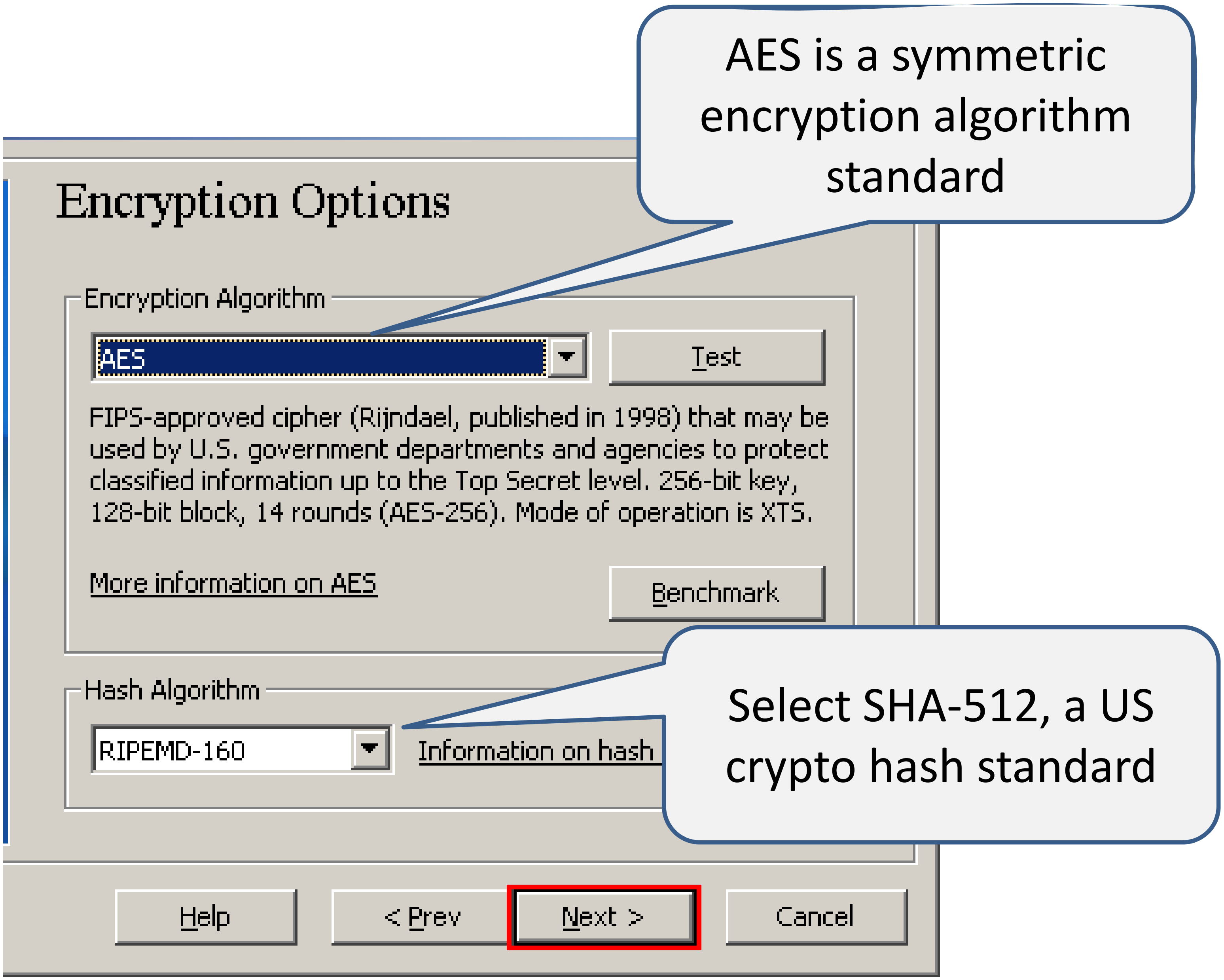
## Volume Location

D:\My Documents\My Volume

☑ 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, copied and 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 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.



Encryption Options

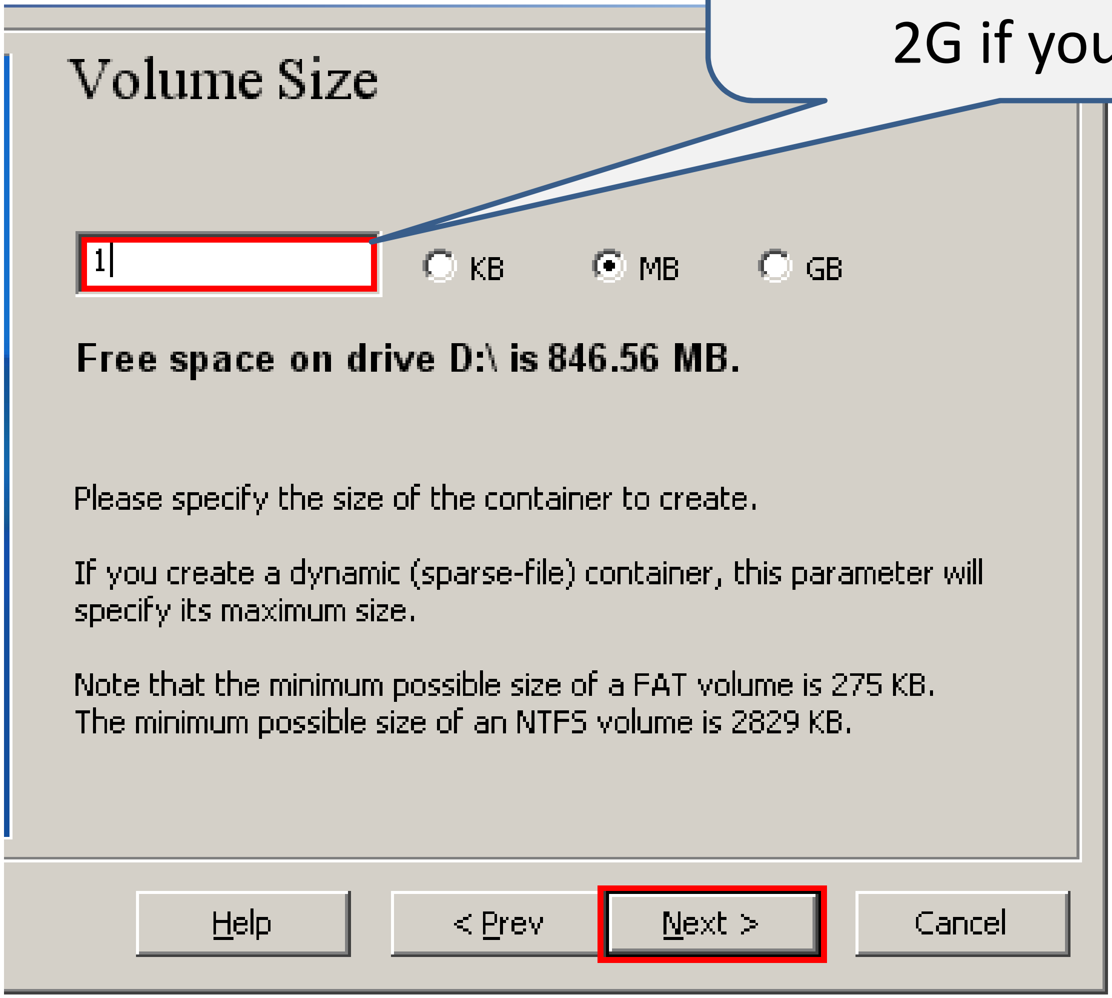
Encryption Algorithm: AES

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.

Hash Algorithm: RIPEMD-160

AES is a symmetric encryption algorithm standard

Select SHA-512, a US crypto hash standard



## Volume Size

1 ○ KB ● MB ○ GB

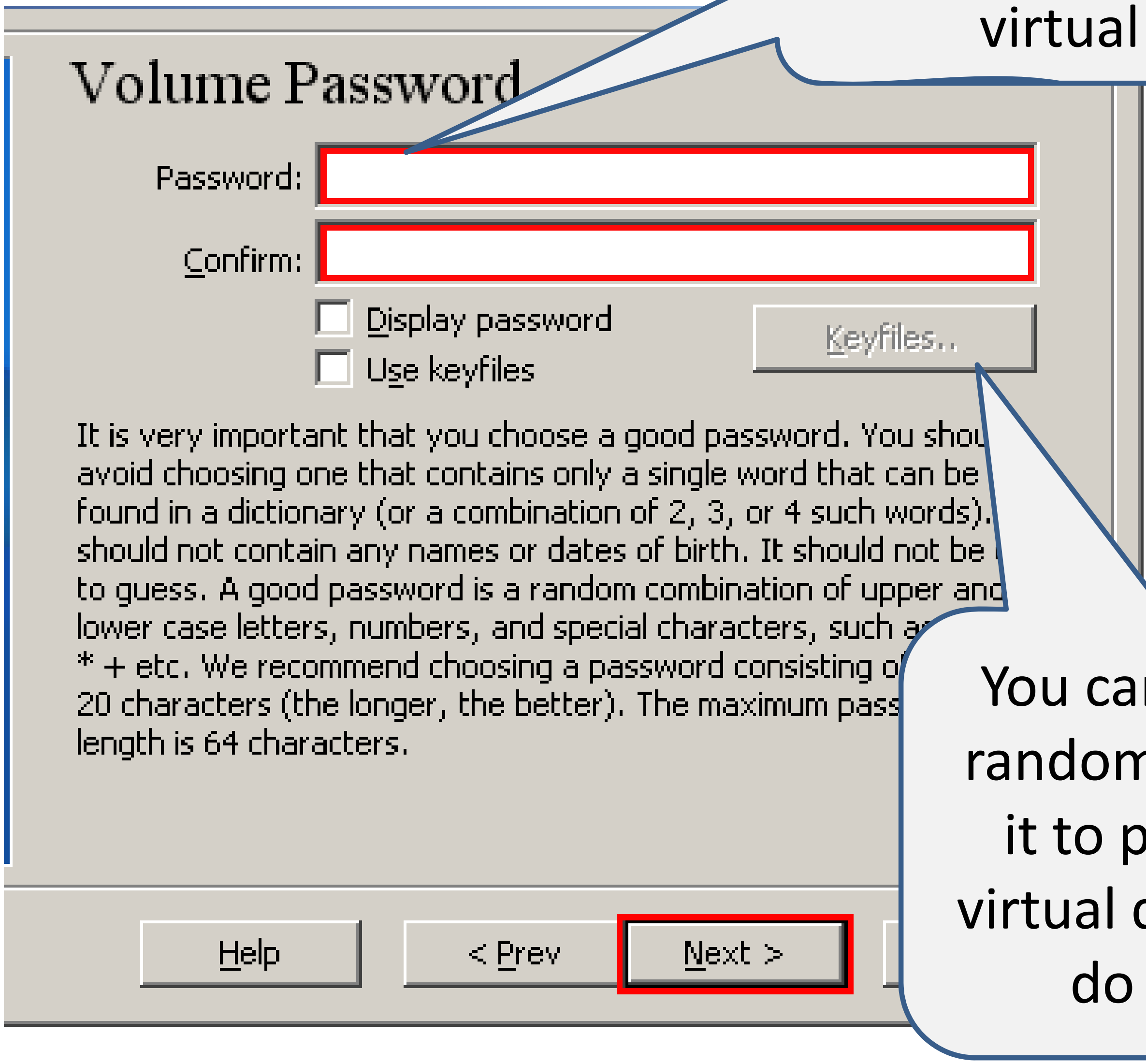
**Free space on drive D:\ is 846.56 MB.**

Please specify the size of the container to create.

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

Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.

The size of your virtual encrypted disk; Choose 2G if you like



Volume Password

Password:

Confirm:

□ Display password

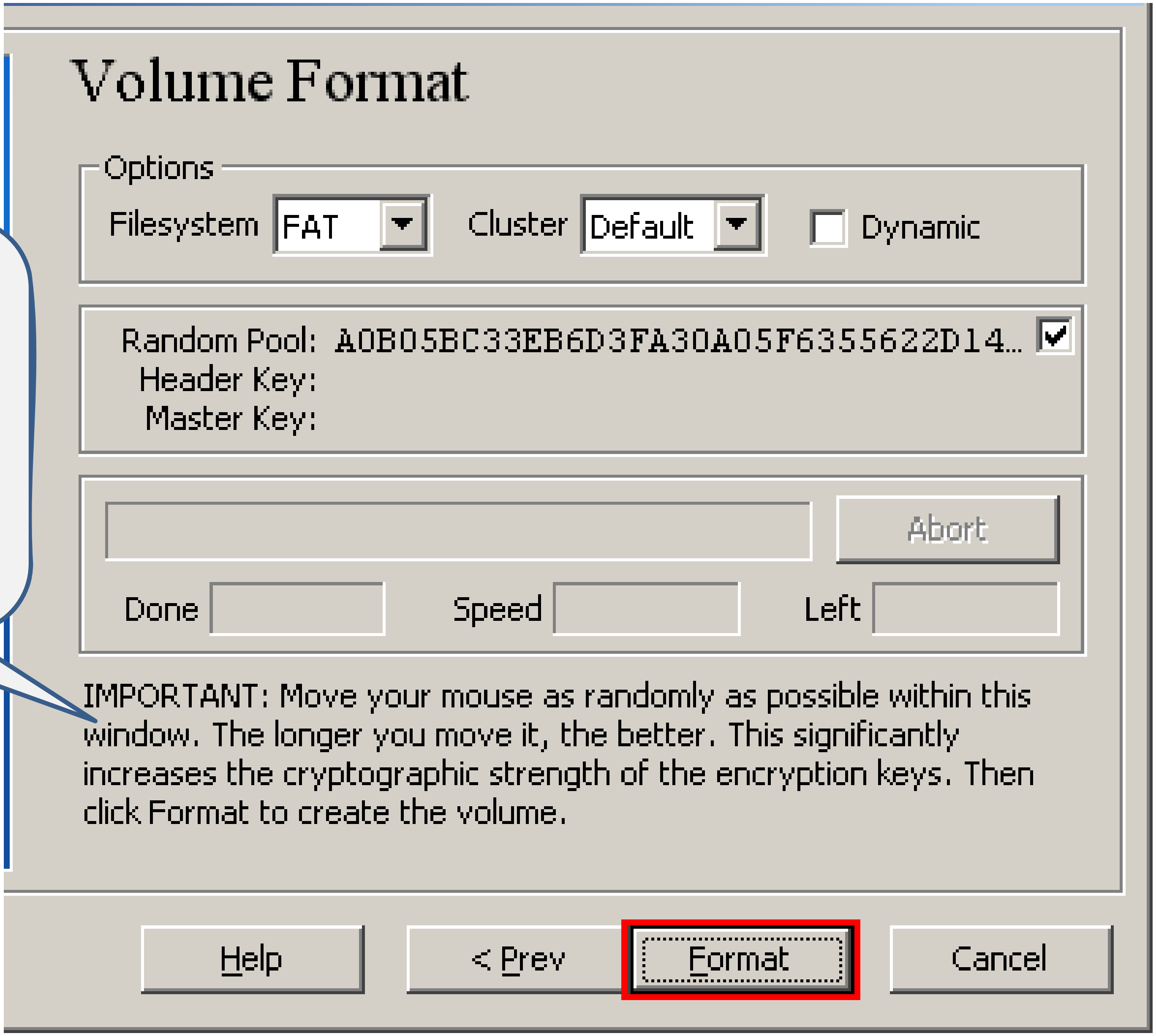
□ Use keyfiles

It is very important that you choose a good password. You shou
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).
should not contain any names or dates of birth. It should not be
to guess. A good password is a random combination of upper and
lower case letters, numbers, and special characters, such a
* + etc. We recommend choosing a password consisting o
20 characters (the longer, the better). The maximum pass
length is 64 characters.

This is the password used to protect your virtual disk

You can generate a random key and use it to protect your virtual disk. Let's **not** do this now

Move your mouse around for 10 seconds to generate some random bits



Volume Format

Options

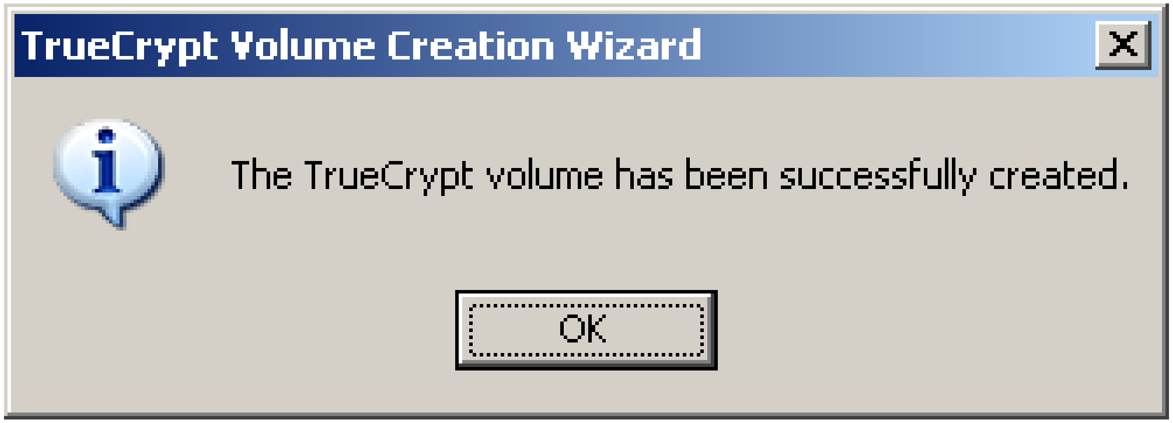
Filesystem FAT

Cluster Default

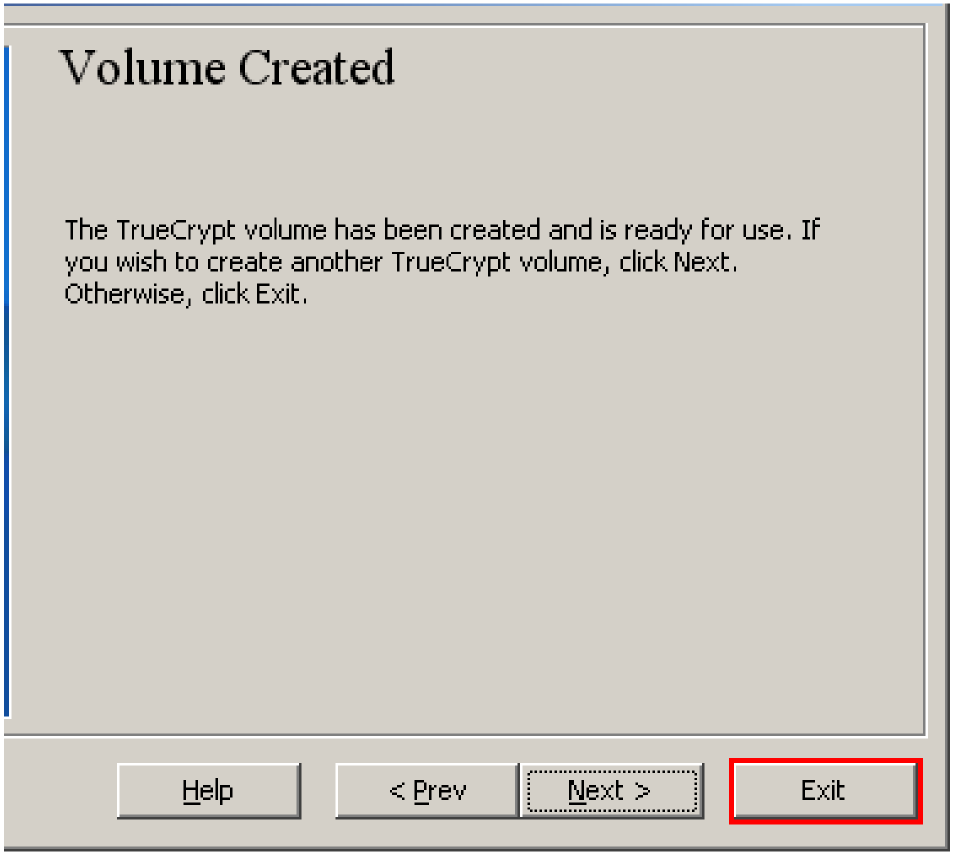
□ Dynamic

Random Pool: A0B05BC33EB6D3FA30A05F6355622D14… ☑
Header Key:
Master Key:

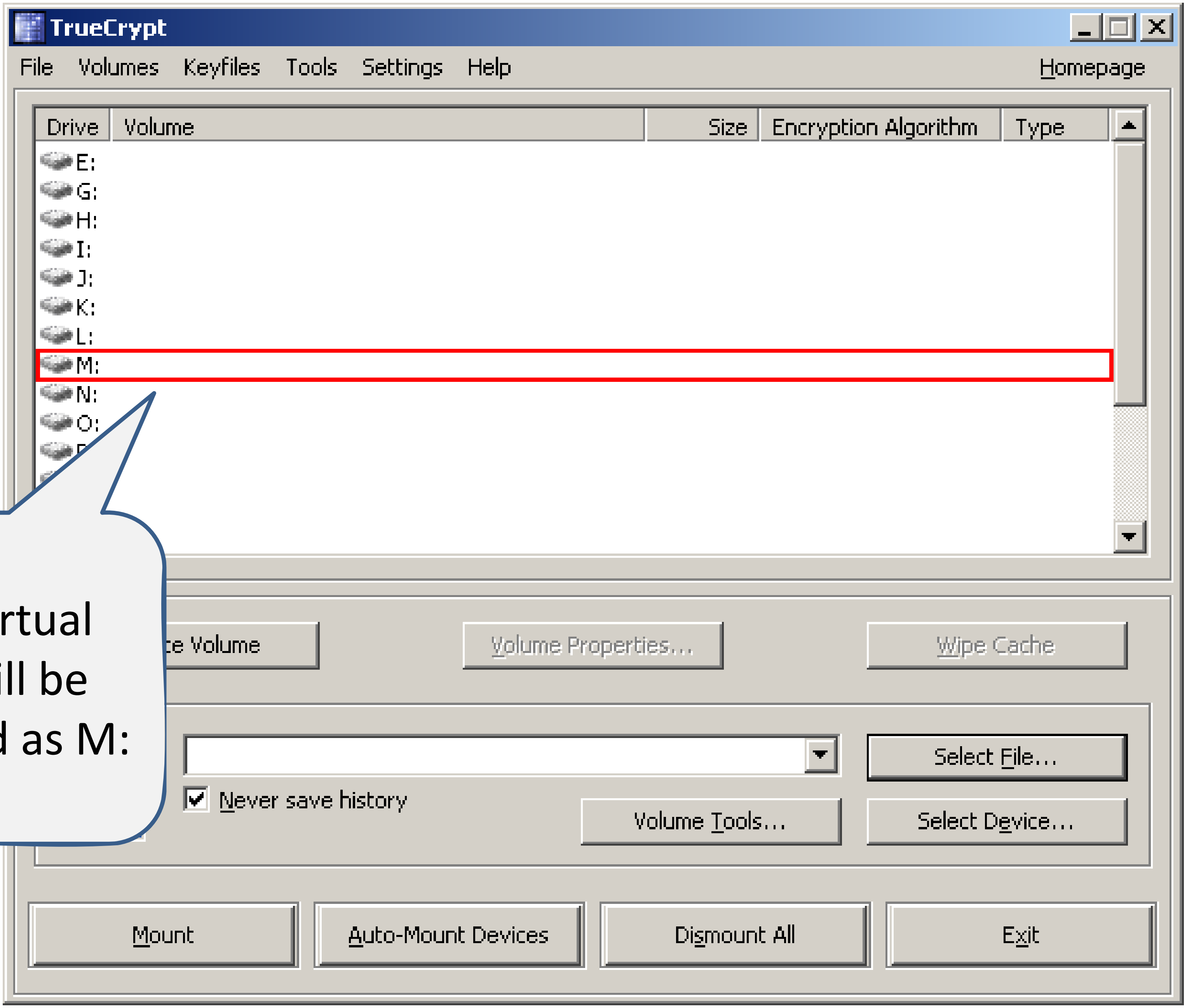
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.



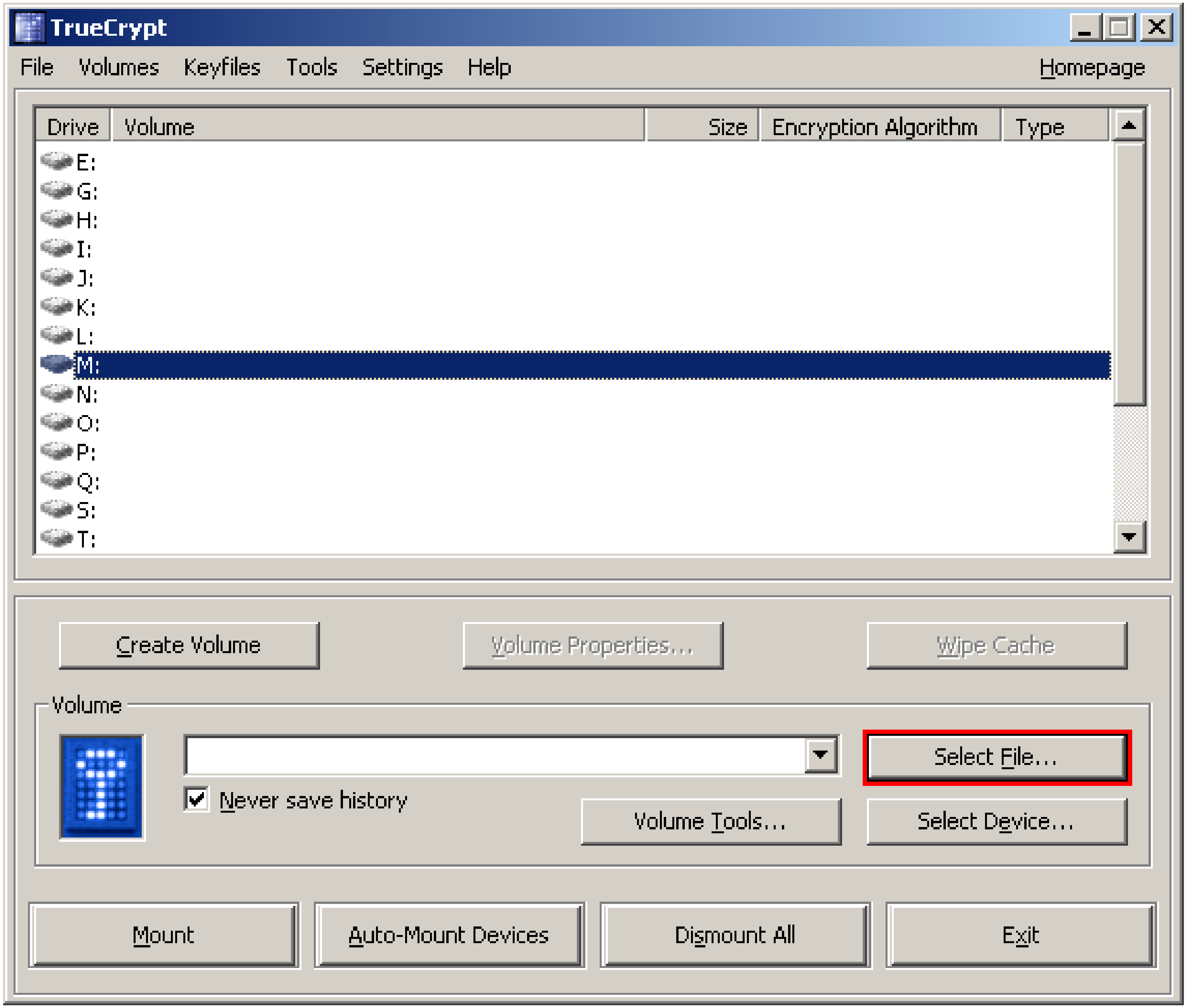
The TrueCrypt volume has been successfully created.



The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.

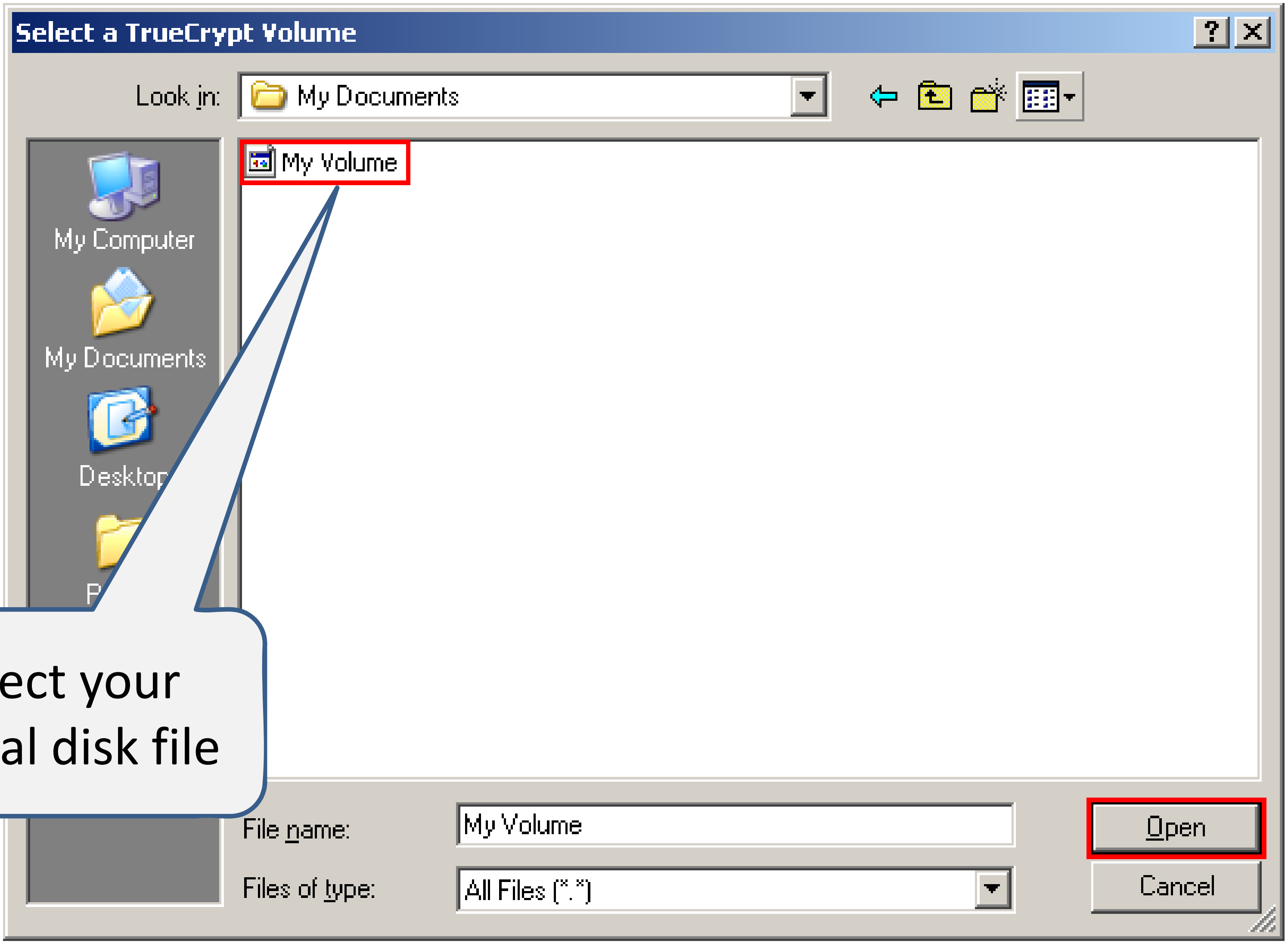


Your virtual disk will be mounted as M:



| Drive | Volume | Size | Encryption Algorithm | Type |
|---|---|---|---|---|
| E: | | | | |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | | | | |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| S: | | | | |
| T: | | | | |

☑ Never save history



Select a TrueCrypt Volume

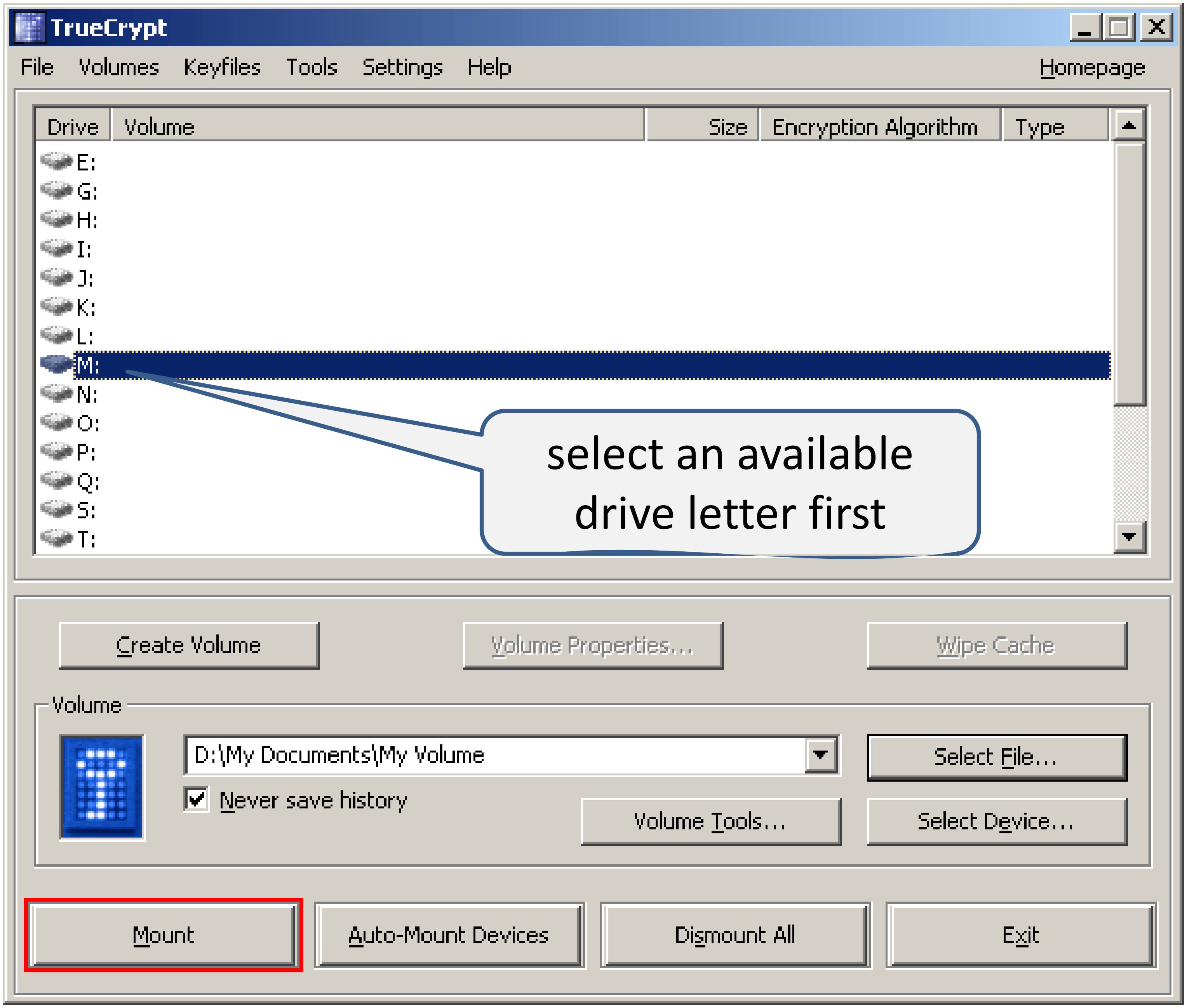
Look in: My Documents

My Volume

File name: My Volume

Files of type: All Files (*.*)

select your virtual disk file

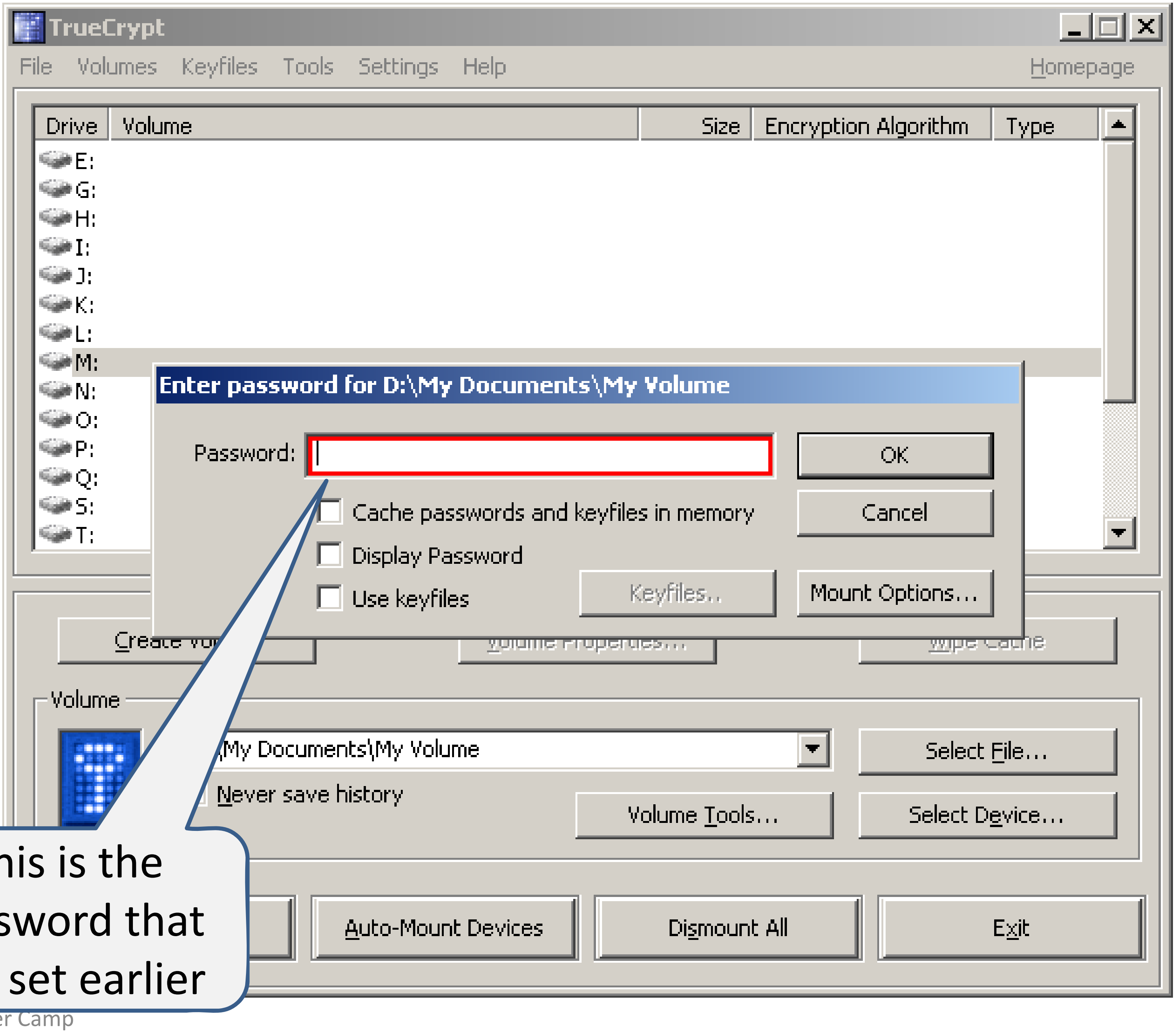


| Drive | Volume | Size | Encryption Algorithm | Type |
|---|---|---|---|---|
| E: | | | | |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | | | | |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| S: | | | | |
| T: | | | | |

Volume: D:\My Documents\My Volume

☑ Never save history

select an available drive letter first



Enter password for D:\My Documents\My Volume

Password:

☐ Cache passwords and keyfiles in memory

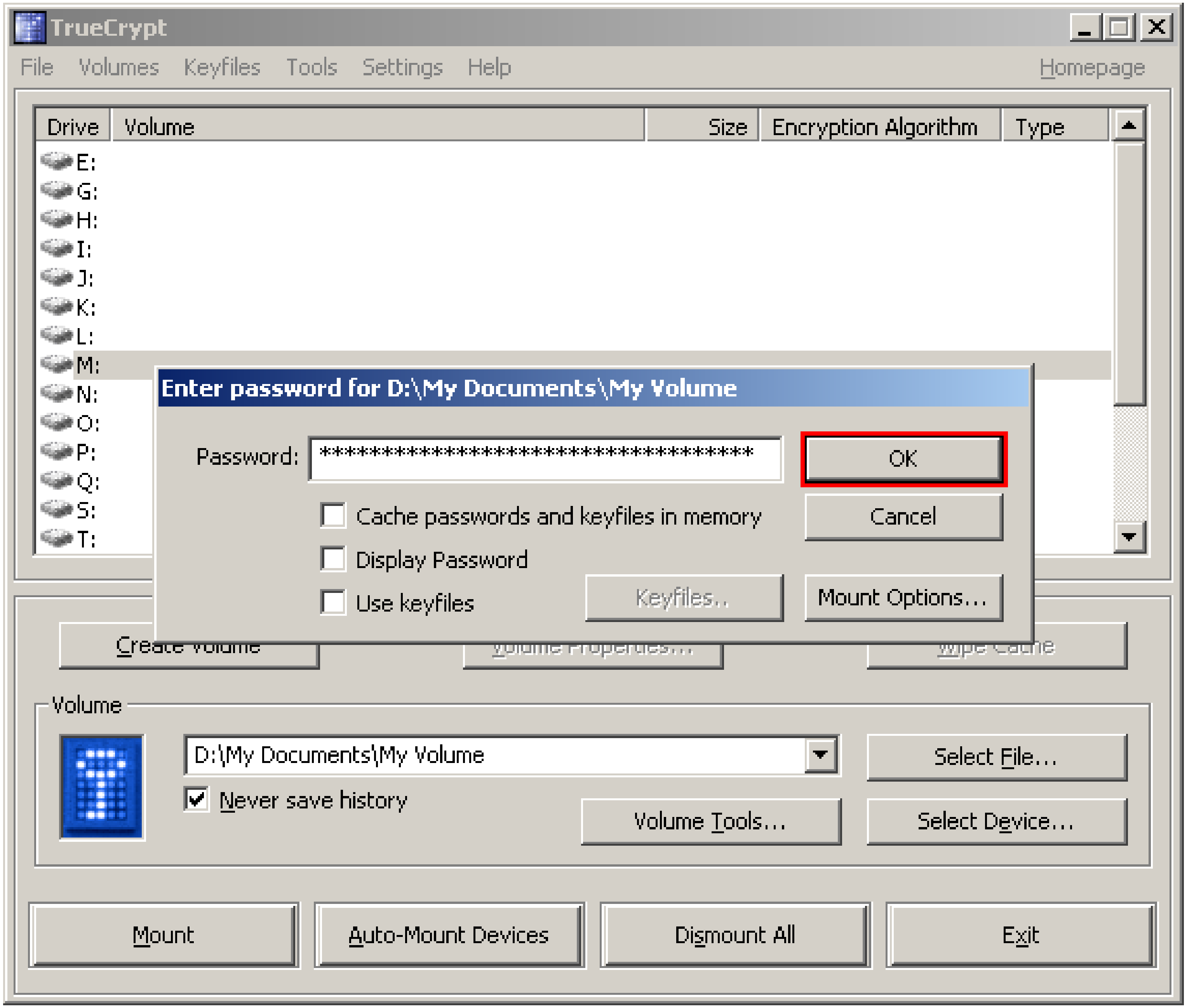
☐ Display Password

☐ Use keyfiles

Volume: \My Documents\My Volume

☐ Never save history

This is the password that you set earlier



| Drive | Volume | Size | Encryption Algorithm | Type |
|---|---|---|---|---|
| E: | | | | |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | | | | |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| S: | | | | |
| T: | | | | |

Enter password for D:\My Documents\My Volume

Password: ************************************

☐ Cache passwords and keyfiles in memory

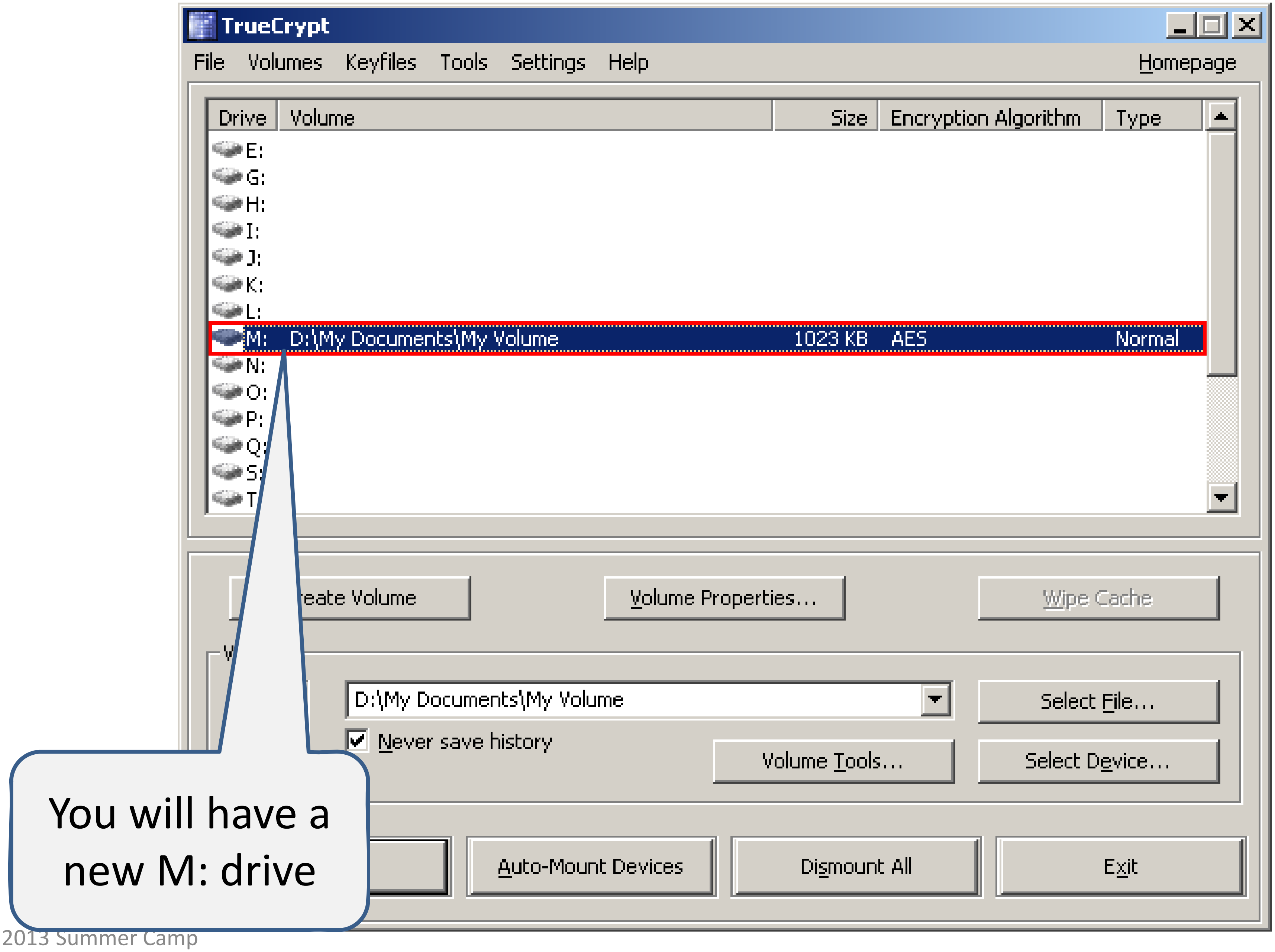
☐ Display Password

☐ Use keyfiles

Volume

D:\My Documents\My Volume

☑ Never save history

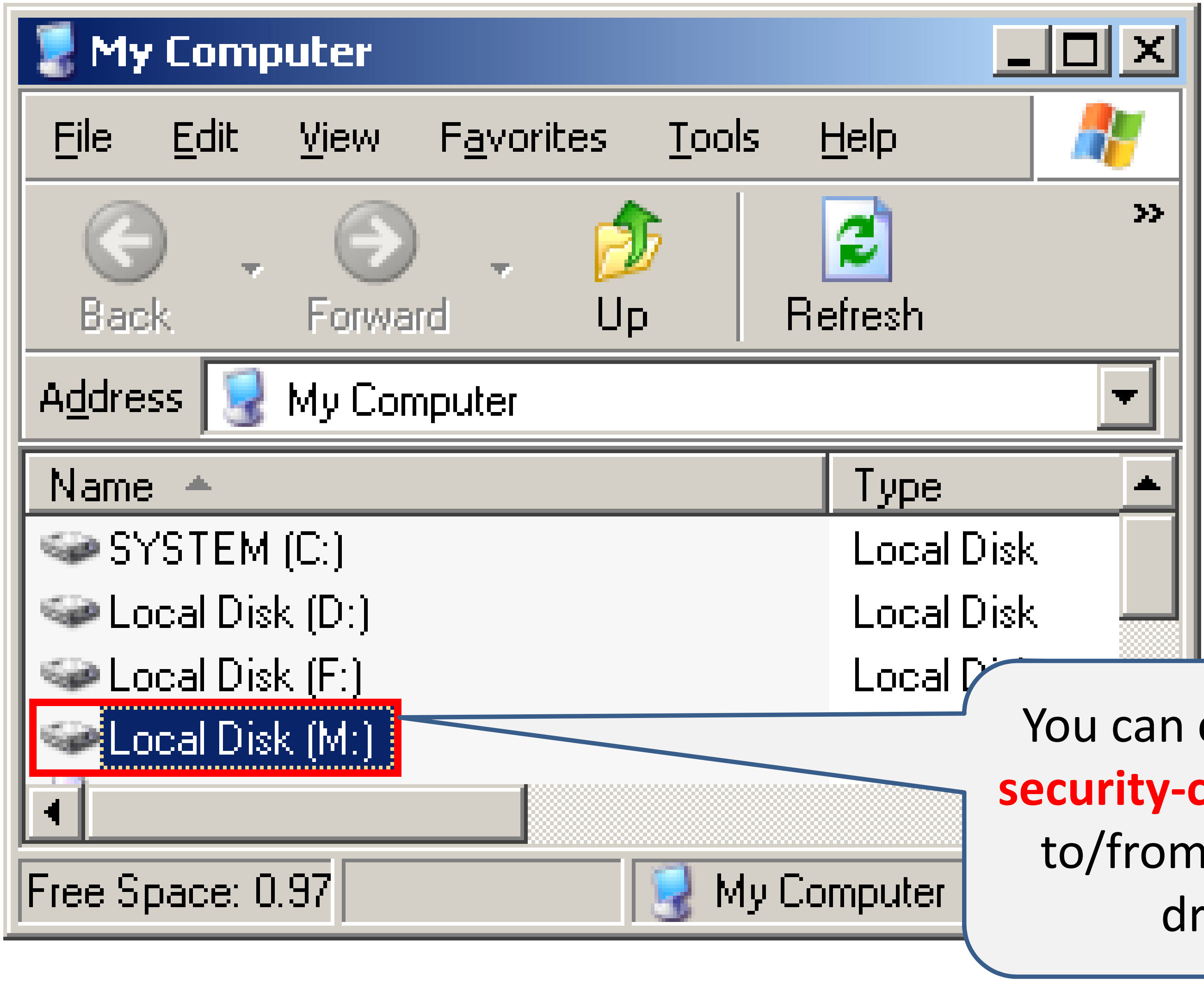


| Drive | Volume | Size | Encryption Algorithm | Type |
|---|---|---|---|---|
| E: | | | | |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | D:\My Documents\My Volume | 1023 KB | AES | Normal |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| S: | | | | |
| T | | | | |

D:\My Documents\My Volume

☑ Never save history

You will have a new M: drive



Address: My Computer

| Name | Type |
|---|---|
| SYSTEM (C:) | Local Disk |
| Local Disk (D:) | Local Disk |
| Local Disk (F:) | Local D |
| Local Disk (M:) | |

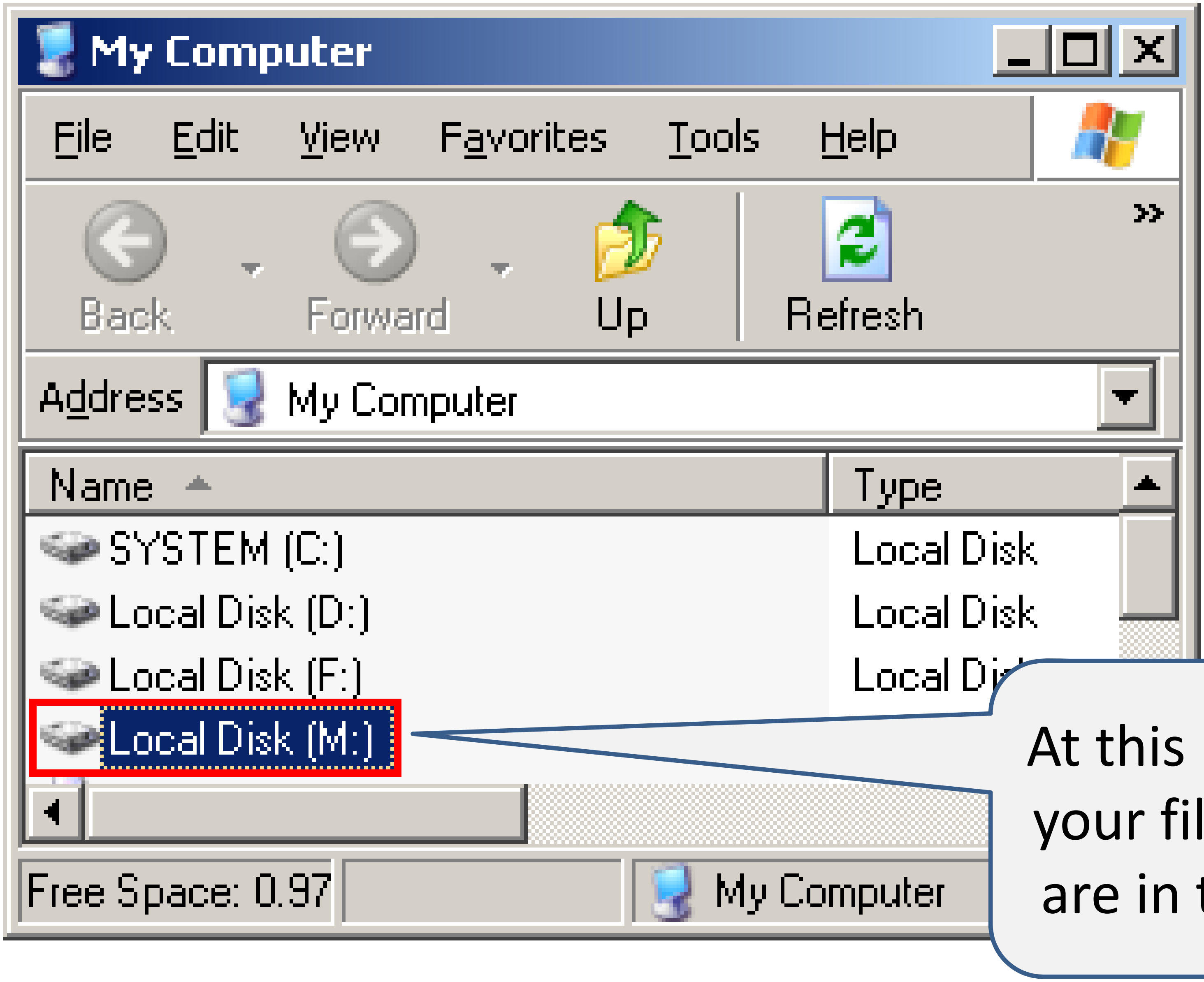
Free Space: 0.97

My Computer

You can copy your **security-critical** files to/from your M: drive

# Security-critical Files?

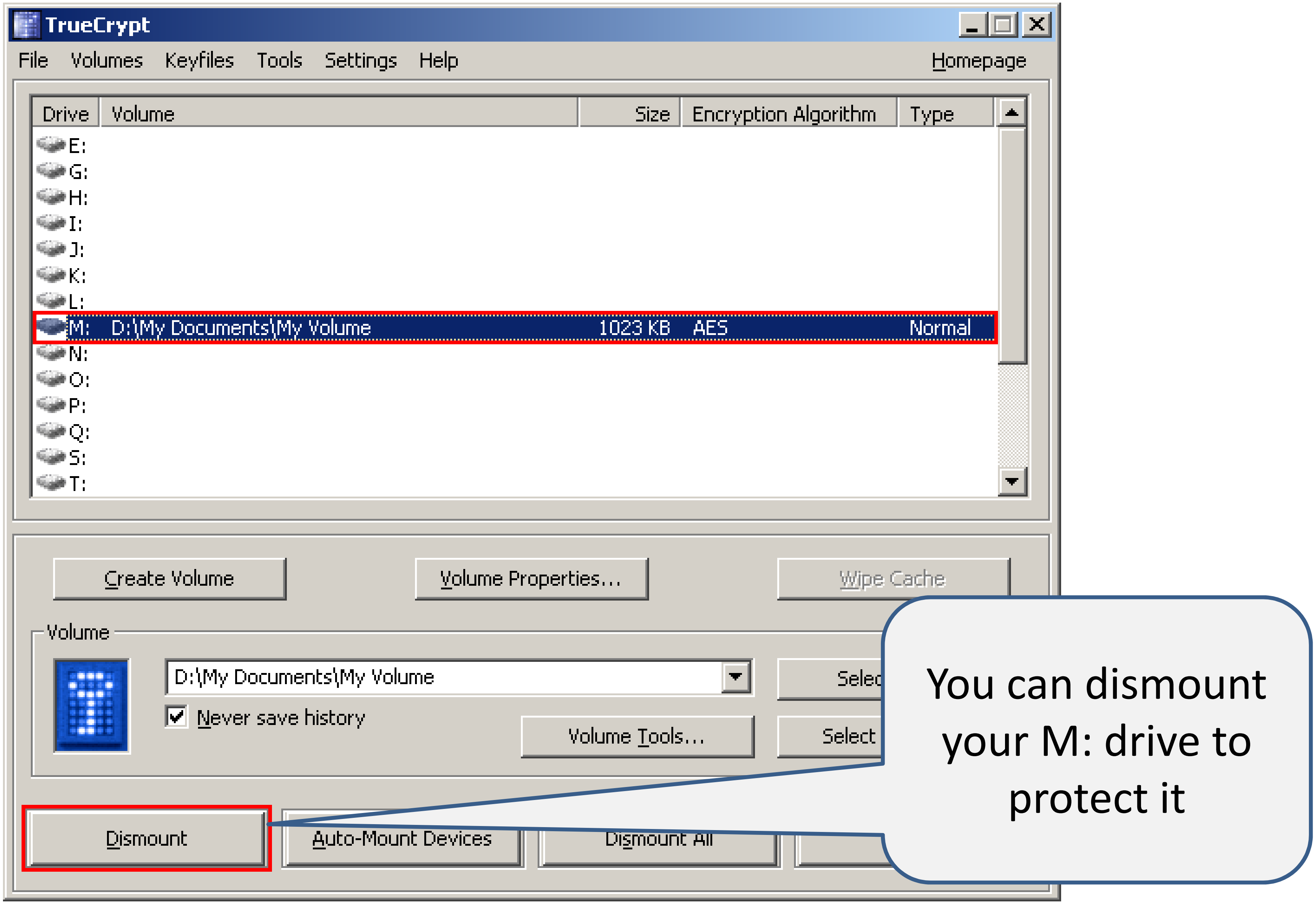
- Create a security-critical text file, finance.txt
  - Save the following information to it
    - your SSN and credit numbers in it
    - Your online banking account information
    - Your utility bill accounts information
    - Your other “important” digital stuffs
- Save it to **M:** drive



Address: My Computer

| Name | Type |
|---|---|
| SYSTEM (C:) | Local Disk |
| Local Disk (D:) | Local Disk |
| Local Disk (F:) | Local Di |
| Local Disk (M:) | |

At this moment, your files on M: are in the clear



| Drive | Volume | Size | Encryption Algorithm | Type |
|---|---|---|---|---|
| E: | | | | |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| K: | | | | |
| L: | | | | |
| M: | D:\My Documents\My Volume | 1023 KB | AES | Normal |
| N: | | | | |
| O: | | | | |
| P: | | | | |
| Q: | | | | |
| S: | | | | |
| T: | | | | |

D:\My Documents\My Volume

☑ Never save history

You can dismount your M: drive to protect it

# Exercise

❶ Create a TrueCrypt virtual disk (filename: *your_first_name-last_name*)

❷ Create a text file, finance.txt, and save it to your virtual disk

❸ Dismount your virtual disk

❹ Examine file *your_first_name-last_name* to see whether you can find any information about finance.txt

❺ Copy *your_first_name-last_name* to c:\tmp

❻ Mount c:\tmp\ *your_first_name-last_name* (the new copy)

❼ Open finance.txt

# Is It Really Secure?

- You can examine your virtual disk file

- If a hacker has stolen your virtual disk file, he/she will not be able to see your critical files

# Do You Really Know What You are Doing?

Warning

- If you pick a strong password and forget it, you will NOT be able to recover any data on the virtual disk
  - Probably nobody will be able to help you
- Know your risk!

# Road Map

- Practice
  - Truecrypt
  - GPG

# Cryptography ≠ Encryption

- Public-key cryptography can be used for digital signature
- The digital counterpart of hand-written signature

# Digital Signature

- Alice uses her private key to digitally sign a message (a bit string)
  - Everybody can use Alice’s public key to verify Alice’s digital signature
- Algorithm buzzwords
  - RSA digital signature
  - Digital Signature Standard (DSS)
  - Elliptic-curve digital signature algorithm (ECDSA)
- (Do not confuse digital signature with email signature in MS Outlook!)

# E-mail signature vs. Digital Signature

- E-mail signature

  Xunhua Wang, PhD
  Department of Computer Science
  James Madison University
  E-mail: wangxx@jmu.edu
  Tel: 540-568-3668

This is **not** secure!
Anybody can change it

- Digital signature

  01110011001…

# What if I Want to…

- Encryption/sign a single file/email?

- GNU Privacy Guard (GPG)
- Windows version
- Gpg4win
  - http://www.gpg4win.org/

# Step 1

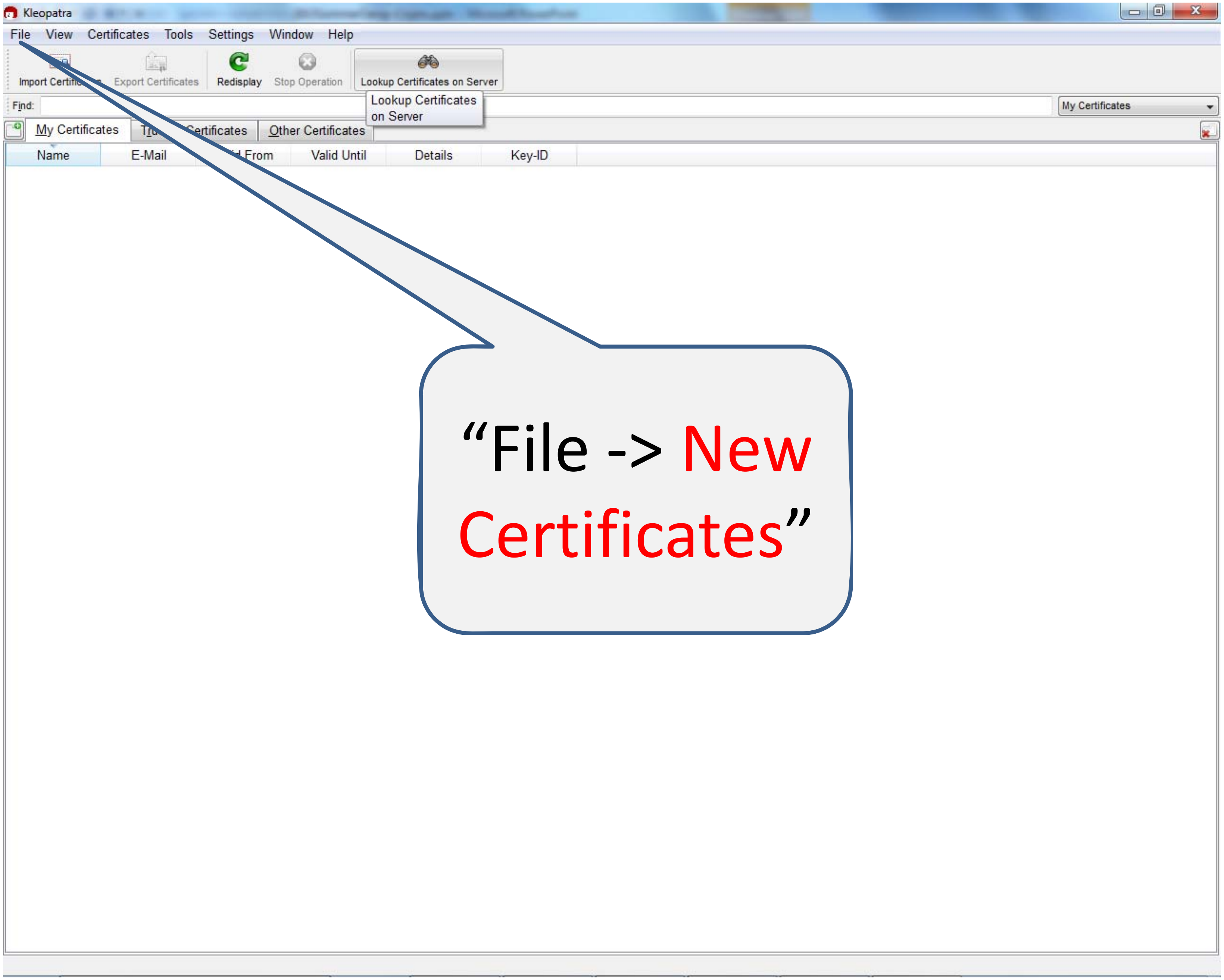
- Download Gpg4win and install it on your Windows 2003 VM
  - http://gpg4win.org/

- NOTE: Gpg4win has already been installed on your Windows 2003 VM under the "**WLAN and Crypto Security**" VM snapshot

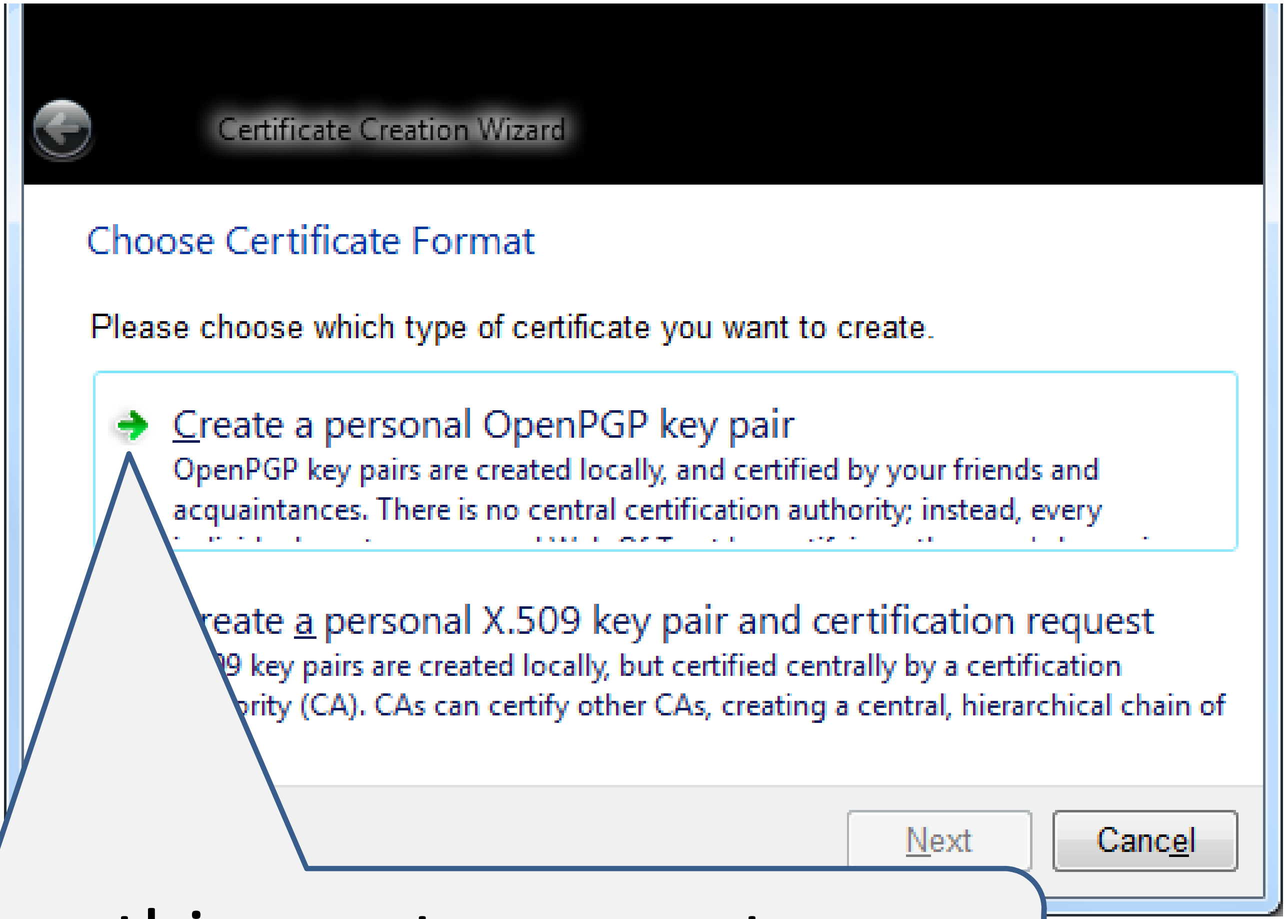
# Step 2

- Run “Start -> All Programs -> Gpg4win -> **Kleopatra**”

- (You can also run it directly from a shortcut on your Desktop)


Kleopatra
File View Certificates Tools Settings Window Help
Import Certificates Export Certificates Redisplay Stop Operation Lookup Certificates on Server
Lookup Certificates on Server
Find:
My Certificates
My Certificates Trusted Certificates Other Certificates
Name E-Mail Valid From Valid Until Details Key-ID

"File -> New Certificates"



Certificate Creation Wizard

Choose Certificate Format

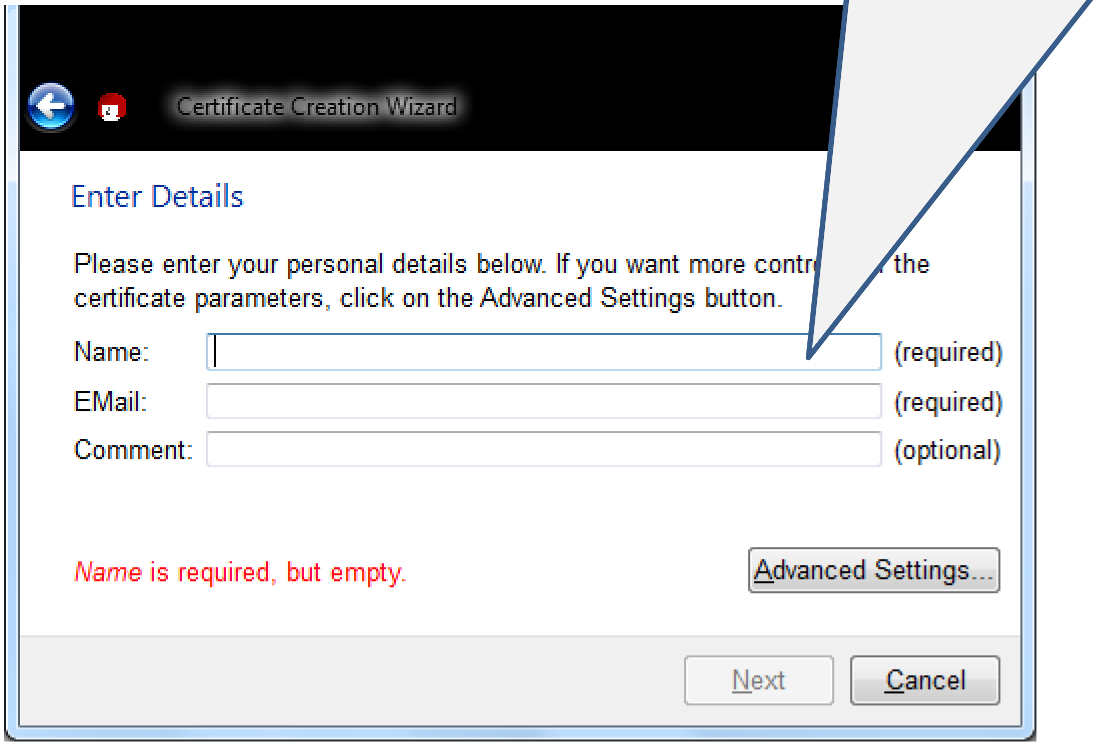
Please choose which type of certificate you want to create.

➔ Create a personal OpenPGP key pair
OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every

reate a personal X.509 key pair and certification request
9 key pairs are created locally, but certified centrally by a certification
ority (CA). CAs can certify other CAs, creating a central, hierarchical chain of

Choose this one to generate your own public/private key pair

Enter the required information



Enter Details

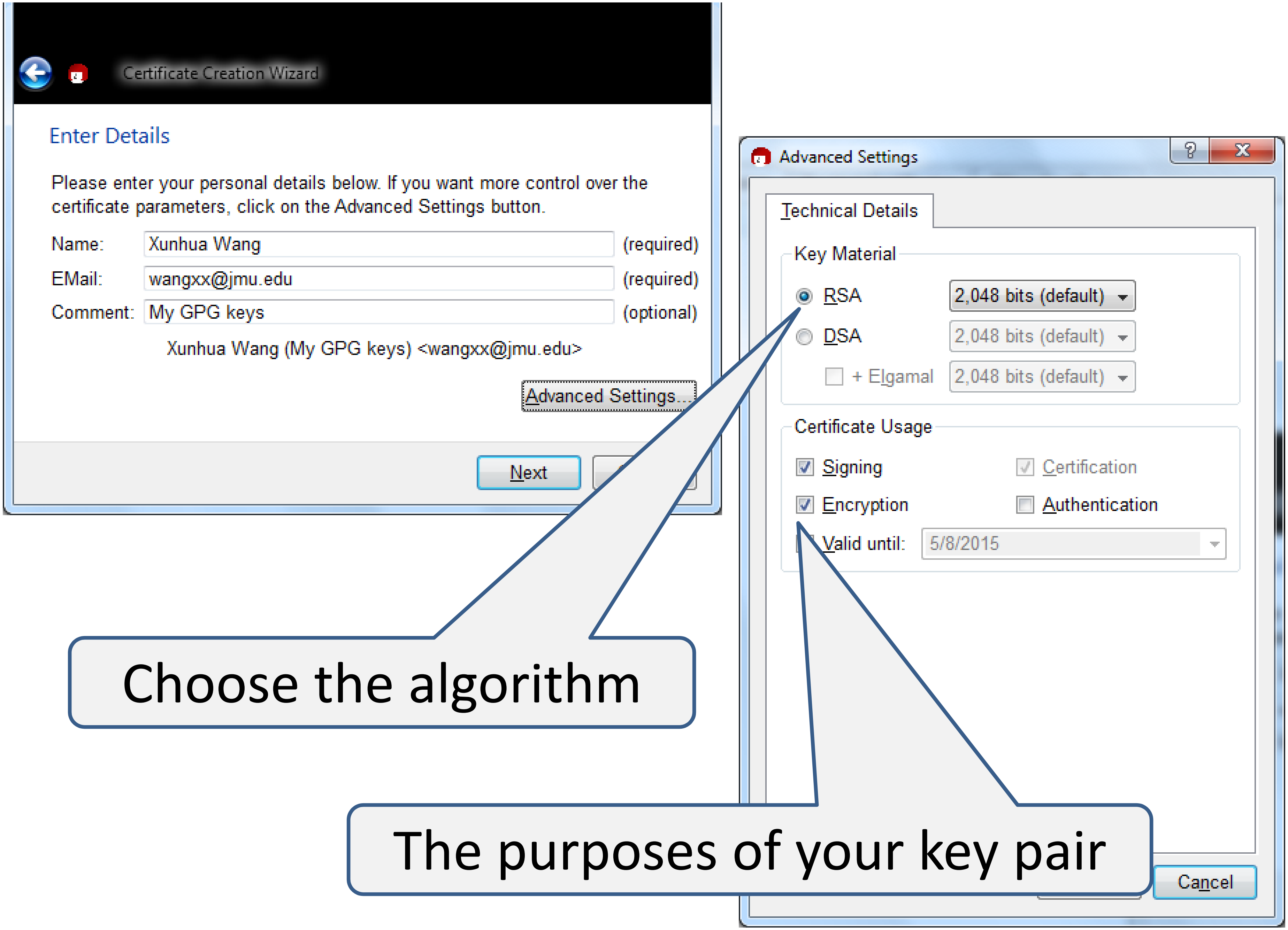
Please enter your personal details below. If you want more contr the certificate parameters, click on the Advanced Settings button.

Name: (required)

EMail: (required)

Comment: (optional)

*Name* is required, but empty.



Enter Details

Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.

| | | |
|---|---|---|
| Name: | Xunhua Wang | (required) |
| EMail: | wangxx@jmu.edu | (required) |
| Comment: | My GPG keys | (optional) |

Xunhua Wang (My GPG keys) <wangxx@jmu.edu>

Key Material

● RSA 2,048 bits (default)

○ DSA 2,048 bits (default)

□ + Elgamal 2,048 bits (default)

Certificate Usage

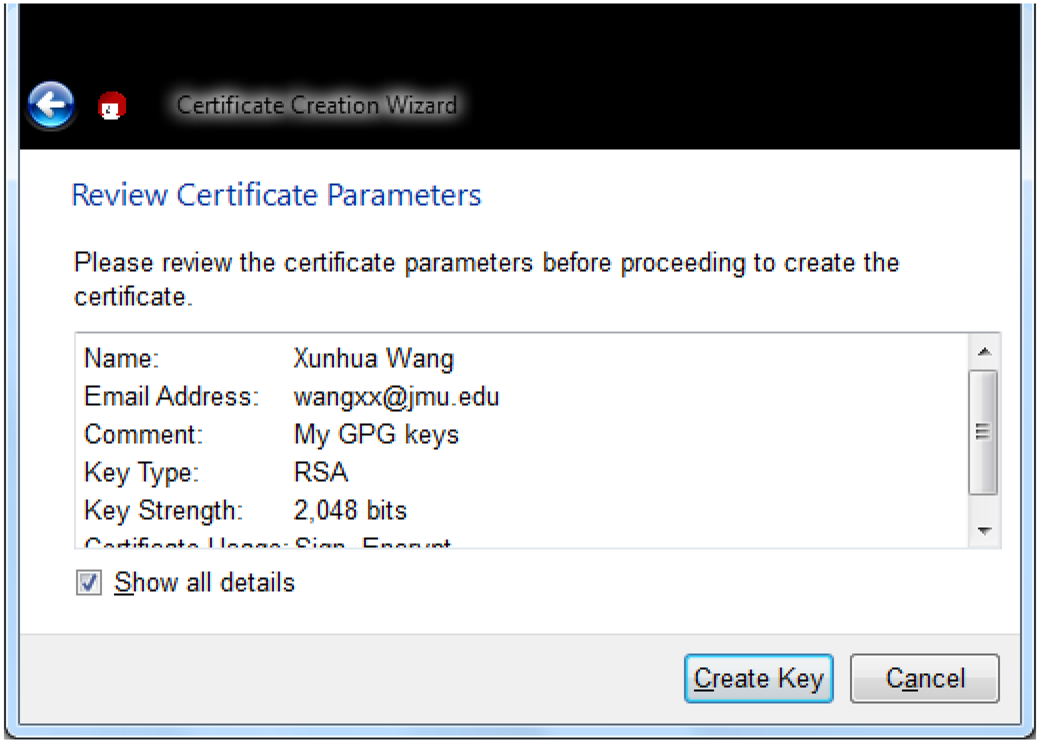
☑ Signing ☑ Certification

☑ Encryption □ Authentication

□ Valid until: 5/8/2015

Choose the algorithm

The purposes of your key pair

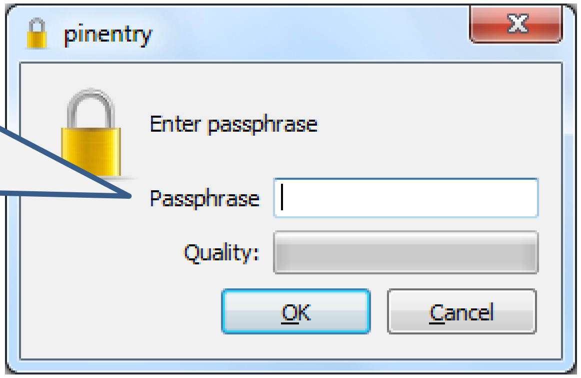


Review Certificate Parameters

Please review the certificate parameters before proceeding to create the certificate.

| | |
|---|---|
| Name: | Xunhua Wang |
| Email Address: | wangxx@jmu.edu |
| Comment: | My GPG keys |
| Key Type: | RSA |
| Key Strength: | 2,048 bits |
| Certificate Usage: | Sign, Encrypt |

☑ Show all details



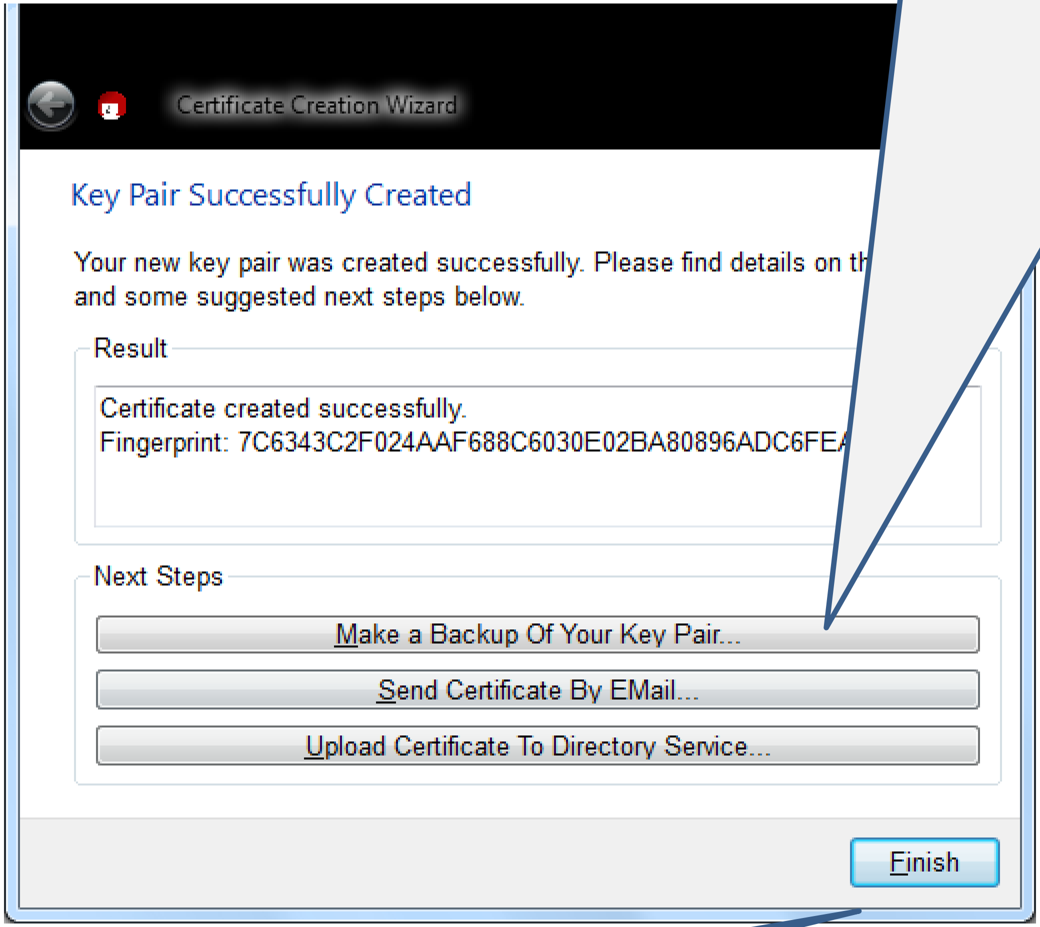
Enter passphrase

Passphrase

Quality:

Choose a password to protect your **private** key

Click this to back up your **private** key to a file (see next slide)


Certificate Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on th
and some suggested next steps below.

Result

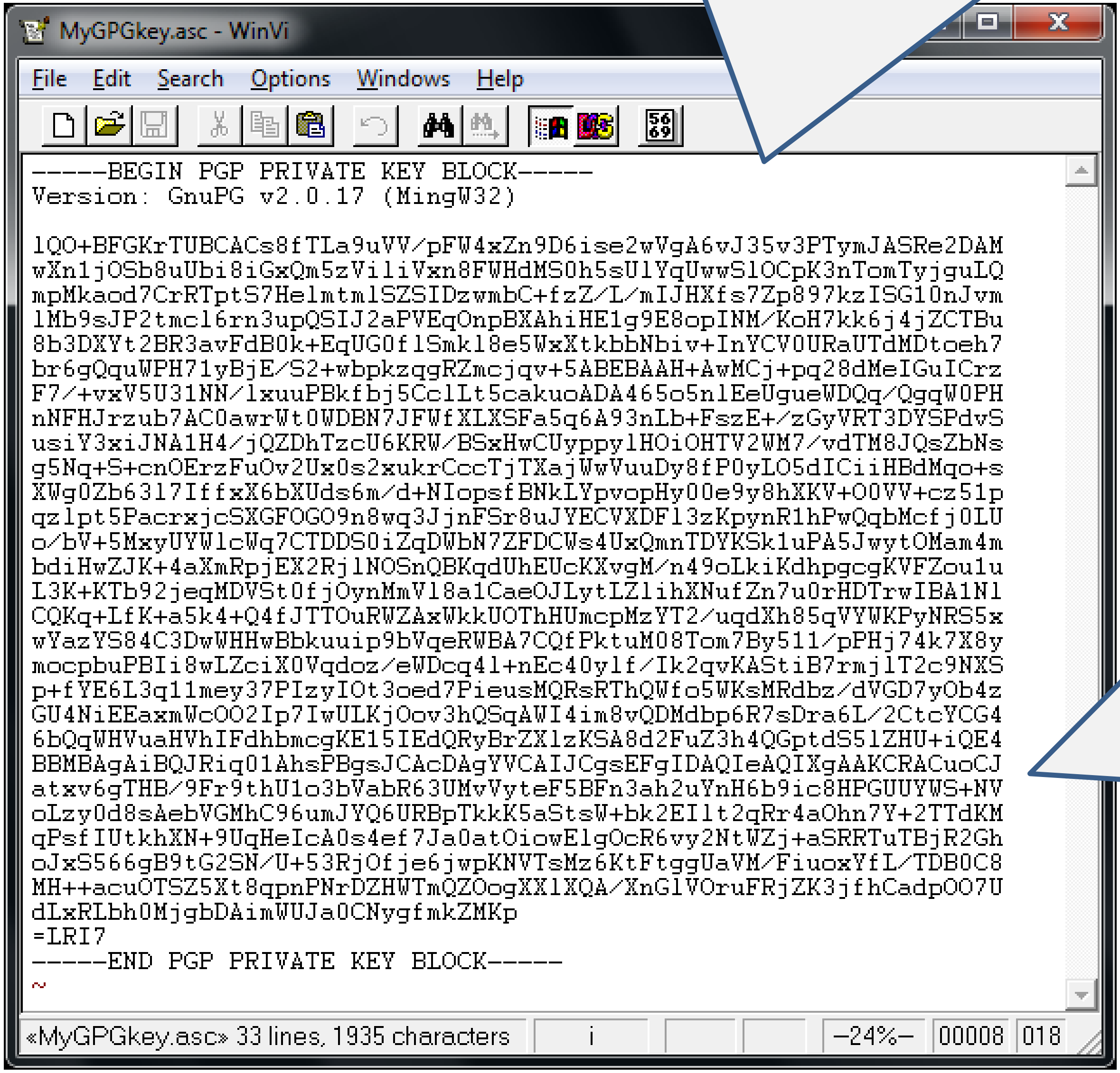
Certificate created successfully.
Fingerprint: 7C6343C2F024AAF688C6030E02BA80896ADC6FEA

Next Steps

Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...
Finish

Everything is cool

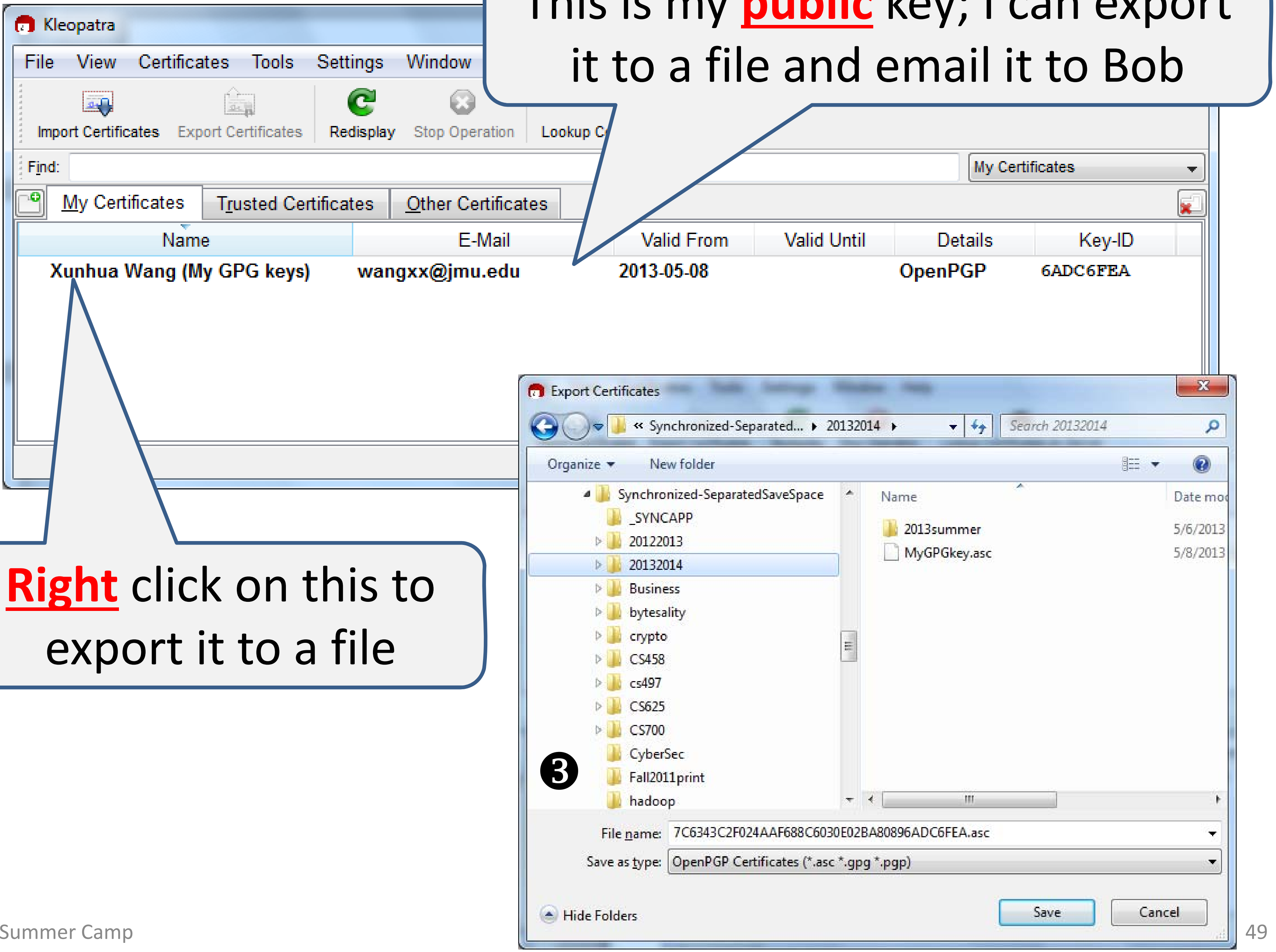
This is your **private** key in a file



```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v2.0.17 (MingW32)

lQO+BFGKrTUBCACs8fTLa9uVV/pFW4xZn9D6ise2wVgA6vJ35v3PTymJASRe2DAM
wXn1jOSb8uUbi8iGxQm5zViliVxn8FWHdMS0h5sUlYqUwwSlOCpK3nTomTyjguLQ
mpMkaod7CrRTptS7HelmtmlSZSIDzwmbC+fzZ/L/mIJHXfs7Zp897kzISG10nJvm
lMb9sJP2tmcl6rn3upQSIJ2aPVEqOnpBXAhiHE1g9E8opINM/KoH7kk6j4jZCTBu
8b3DXYt2BR3avFdB0k+EqUG0flSmkl8e5WxXtkbbNbiv+InYCV0URaUTdMDtoeh7
br6gQquWPH71yBjE/S2+wbpkzqgRZmcjqv+5ABEBAAH+AwMCj+pq28dMeIGuICrz
F7/+vxV5U31NN/lxuuPBkfbj5CclLt5cakuoADA465o5nlEeUgueWDQq/QgqW0PH
nNFHJrzub7AC0awrWt0WDBN7JFWfXLXSFa5q6A93nLb+FszE+/zGyVRT3DYSPdvS
usiY3xiJNA1H4/jQZDhTzcU6KRW/BSxHwCUyppylHOiOHTV2WM7/vdTM8JQsZbNs
g5Nq+S+cnOErzFuOv2Ux0s2xukrCccTjTXajWwVuuDy8fP0yLO5dICiiHBdMqo+s
XWg0Zb6317IffxX6bXUds6m/d+NIopsfBNkLYpvopHy00e9y8hXKV+O0VV+cz51p
qzlpt5PacrxjcSXGFOGO9n8wq3JjnFSr8uJYECVXDFl3zKpynR1hPwQqbMcfj0LU
o/bV+5MxyUYWlcWq7CTDDS0iZqDWbN7ZFDCWs4UxQmnTDYKSk1uPA5JwytOMam4m
bdiHwZJK+4aXmRpjEX2RjlNOSnQBKqdUhEUcKXvgM/n49oLkiKdhpgcgKVFZou1u
L3K+KTb92jeqMDVSt0fjOynMmVl8a1CaeOJLytLZlihXNufZn7u0rHDTrwIBA1Nl
CQKq+LfK+a5k4+Q4fJTTOuRWZAxWkkUOThHUmcpMzYT2/uqdXh85qVYWKPyNRS5x
wYazYS84C3DwWHHwBbkuuip9bVqeRWBA7CQfPktuM08Tom7By511/pPHj74k7X8y
mocpbuPBIi8wLZciX0Vqdoz/eWDcq4l+nEc40ylf/Ik2qvKAStiB7rmjlT2c9NXS
p+fYE6L3q1lmey37PIzyIOt3oed7PieusMQRsRThQWfo5WKsMRdbz/dVGD7yOb4z
GU4NiEEaxmWcOO2Ip7IwULKjOov3hQSqAWI4im8vQDMdbp6R7sDra6L/2CtcYCG4
6bQqWHVuaHVhIFdhbmcgKE15IEdQRyBrZXlzKSA8d2FuZ3h4QGptdS5lZHU+iQE4
BBMBAgAiBQJRiq01AhsPBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRACuoCJ
atxv6gTHB/9Fr9thU1o3bVabR63UMvVyteF5BFn3ah2uYnH6b9ic8HPGUUYWS+NV
oLzy0d8sAebVGMhC96umJYQ6URBpTkkK5aStsW+bk2EIlt2qRr4aOhn7Y+2TTdKM
qPsfIUtkhXN+9UqHeIcA0s4ef7Ja0atOiowElgOcR6vy2NtWZj+aSRRTuTBjR2Gh
oJxS566gB9tG2SN/U+53RjOfje6jwpKNVTsMz6KtFtggUaVM/FiuoxYfL/TDB0C8
MH++acuOTSZ5Xt8qpnPNrDZHWTmQZOogXXlXQA/XnGlVOruFRjZK3jfhCadpOO7U
dLxRLbh0MjgbDAimWUJa0CNygfmkZMKp
=LRI7
-----END PGP PRIVATE KEY BLOCK-----
~
```

«MyGPGkey.asc» 33 lines, 1935 characters | i | | | –24%– | 00008 | 018

This is your **private** key, it is supposed to be secret: do **not** lose it or send it to your friend



| Name | E-Mail | Valid From | Valid Until | Details | Key-ID |
|---|---|---|---|---|---|
| Xunhua Wang (My GPG keys) | wangxx@jmu.edu | 2013-05-08 | | OpenPGP | 6ADC6FEA |

| Name | Date mod |
|---|---|
| 2013summer | 5/6/2013 |
| MyGPGkey.asc | 5/8/2013 |

File name: 7C6343C2F024AAF688C6030E02BA80896ADC6FEA.asc

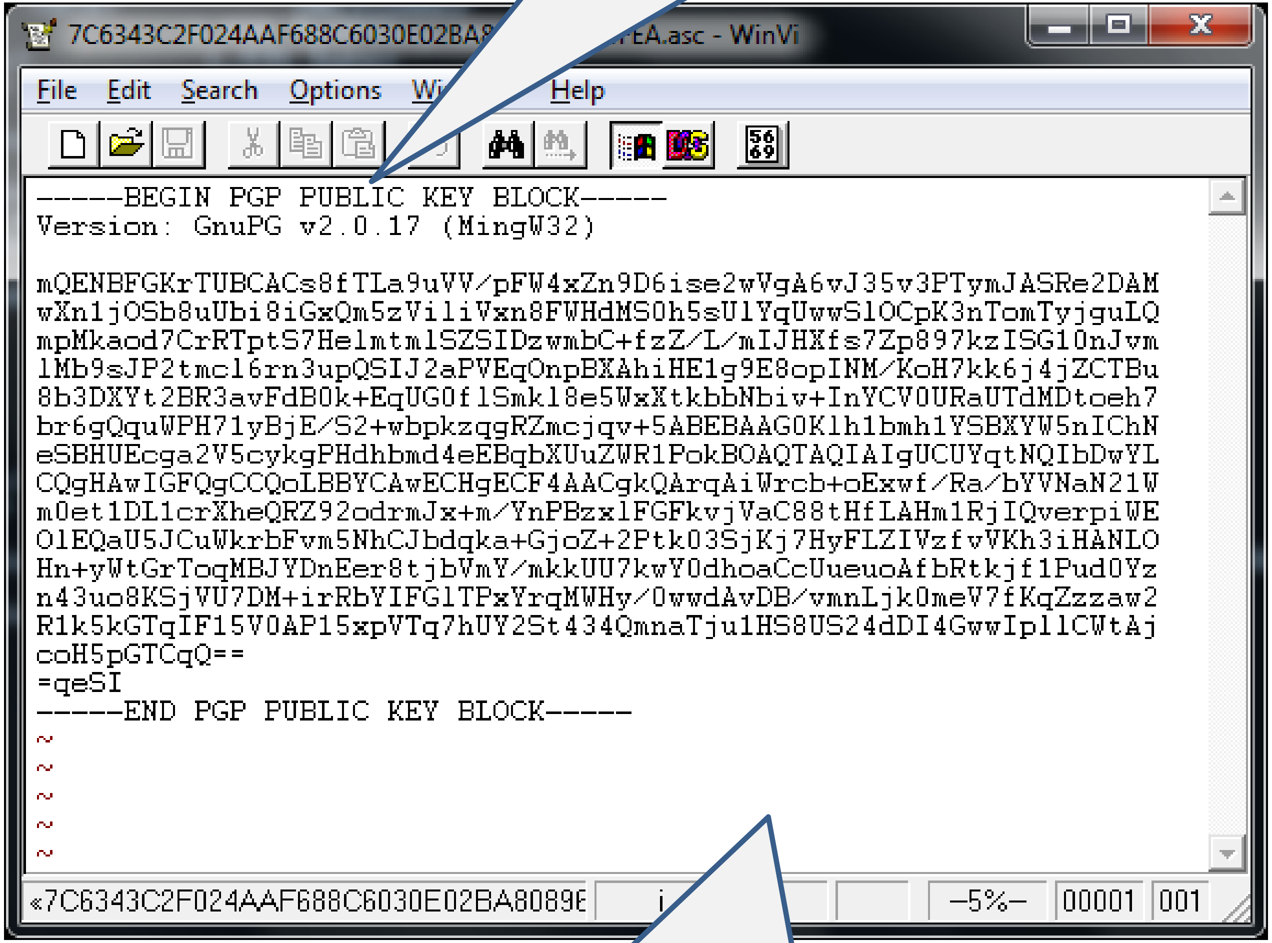
Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)

This is my **public** key; I can export it to a file and email it to Bob

**Right** click on this to export it to a file

❸

This is my **public** key in a file


7C6343C2F024AAF688C6030E02BA8 EA.asc - WinVi
File
Edit
Search
Options
Wi
Help
«7C6343C2F024AAF688C6030E02BA8089E
-5%-
00001
001

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.17 (MingW32)

mQENBFGKrTUBCACs8fTLa9uVV/pFW4xZn9D6ise2wVgA6vJ35v3PTymJASRe2DAM
wXn1jOSb8uUbi8iGxQm5zViliVxn8FWHdMS0h5sUlYqUwwSlOCpK3nTomTyjguLQ
mpMkaod7CrRTptS7HelmtmlSZSIDzwmbC+fzZ/L/mIJHXfs7Zp897kzISG10nJvm
lMb9sJP2tmcl6rn3upQSIJ2aPVEqOnpBXAhiHE1g9E8opINM/KoH7kk6j4jZCTBu
8b3DXYt2BR3avFdB0k+EqUG0flSmkl8e5WxXtkbbNbiv+InYCV0URaUTdMDtoeh7
br6gQquWPH71yBjE/S2+wbpkzqgRZmcjqv+5ABEBAAG0Klh1bmh1YSBXYW5nIChN
eSBHUEcga2V5cykgPHdhbmd4eEBqbXUuZWR1PokBOAQTAQIAIgUCUYqtNQIbDwYL
CQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQArqAiWrcb+oExwf/Ra/bYVNaN21W
m0et1DL1crXheQRZ92odrmJx+m/YnPBzxlFGFkvjVaC88tHfLAHm1RjIQverpiWE
OlEQaU5JCuWkrbFvm5NhCJbdqka+GjoZ+2Ptk03SjKj7HyFLZIVzfvVKh3iHANLO
Hn+yWtGrToqMBJYDnEer8tjbVmY/mkkUU7kwY0dhoaCcUueuoAfbRtkjf1Pud0Yz
n43uo8KSjVU7DM+irRbYIFGlTPxYrqMWHy/0wwdAvDB/vmnLjk0meV7fKqZzzaw2
R1k5kGTqIF15V0AP15xpVTq7hUY2St434QmnaTju1HS8US24dDI4GwwIpllCWtAj
coH5pGTCqQ==
=qeSI
-----END PGP PUBLIC KEY BLOCK-----
~
~
~
~
~
```

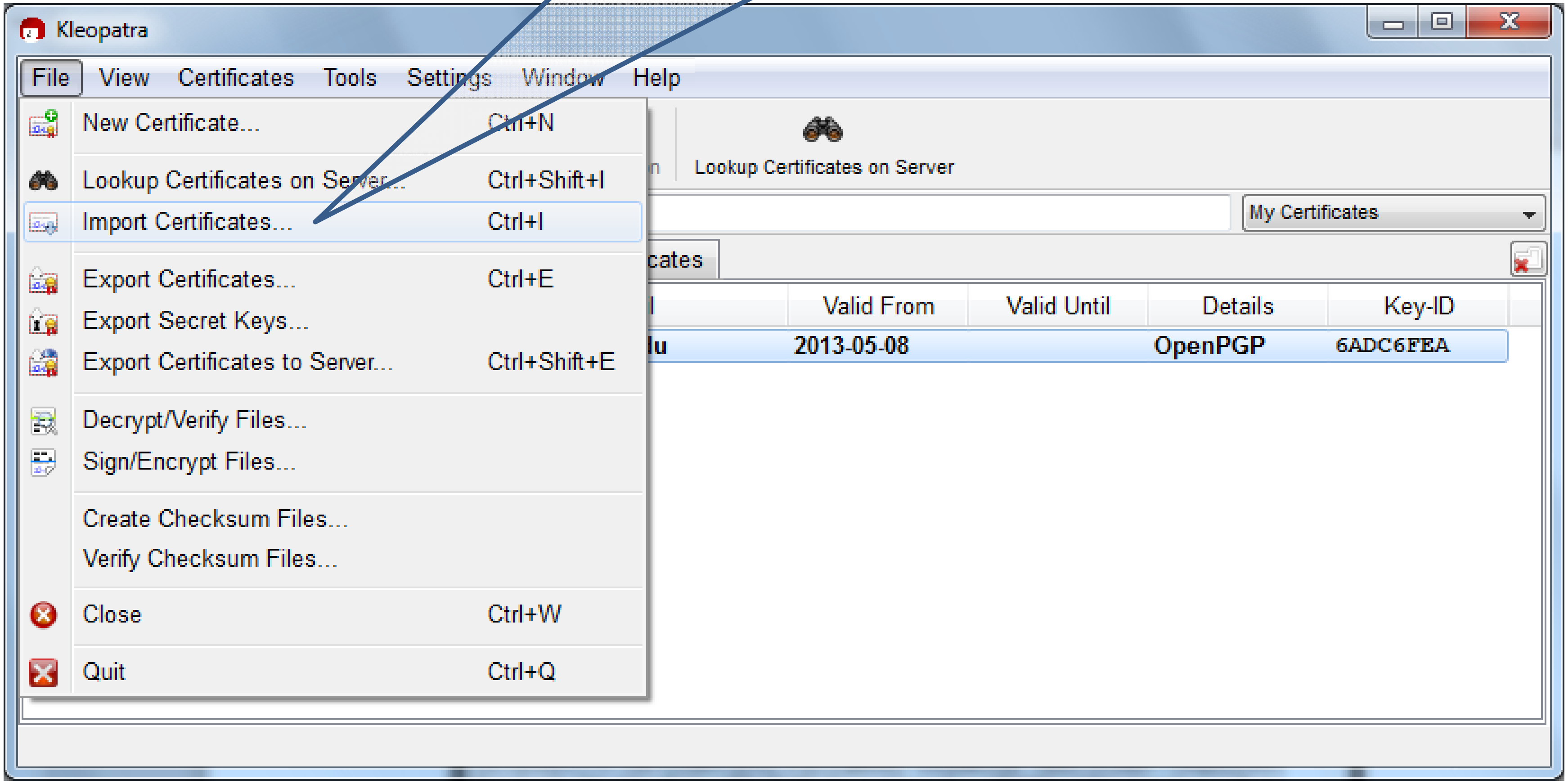
I can email it to my friends

# Exercise #1

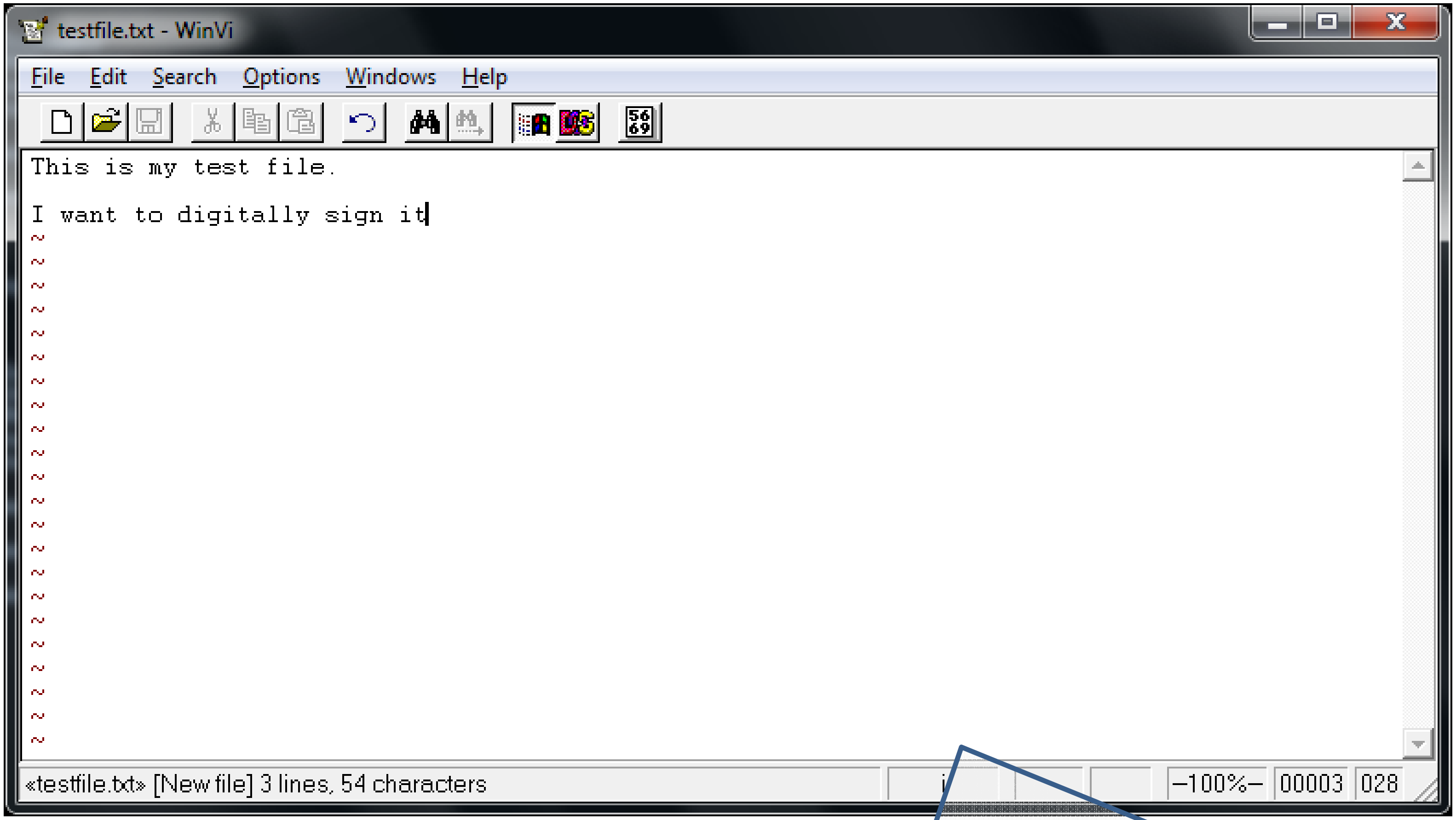
❶Export your **public** key to a file and email it to the student next to you

❷After receiving a public key from your classmate, import it to your Gpg4win (see next slide)

Click “File -> Import Certificates …” to import the public key received from your classmate



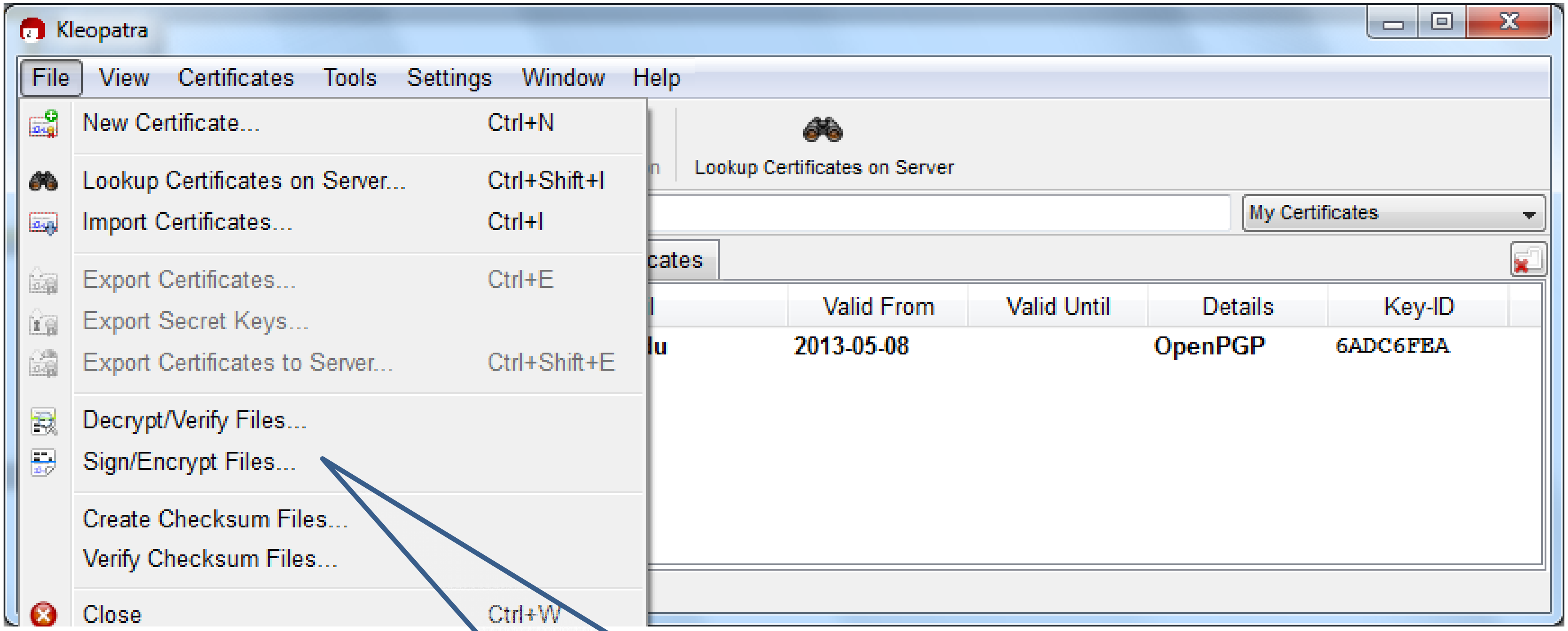
# Now, I Want to digitally Sign a file and Send it to My Friend



```
This is my test file.

I want to digitally sign it
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

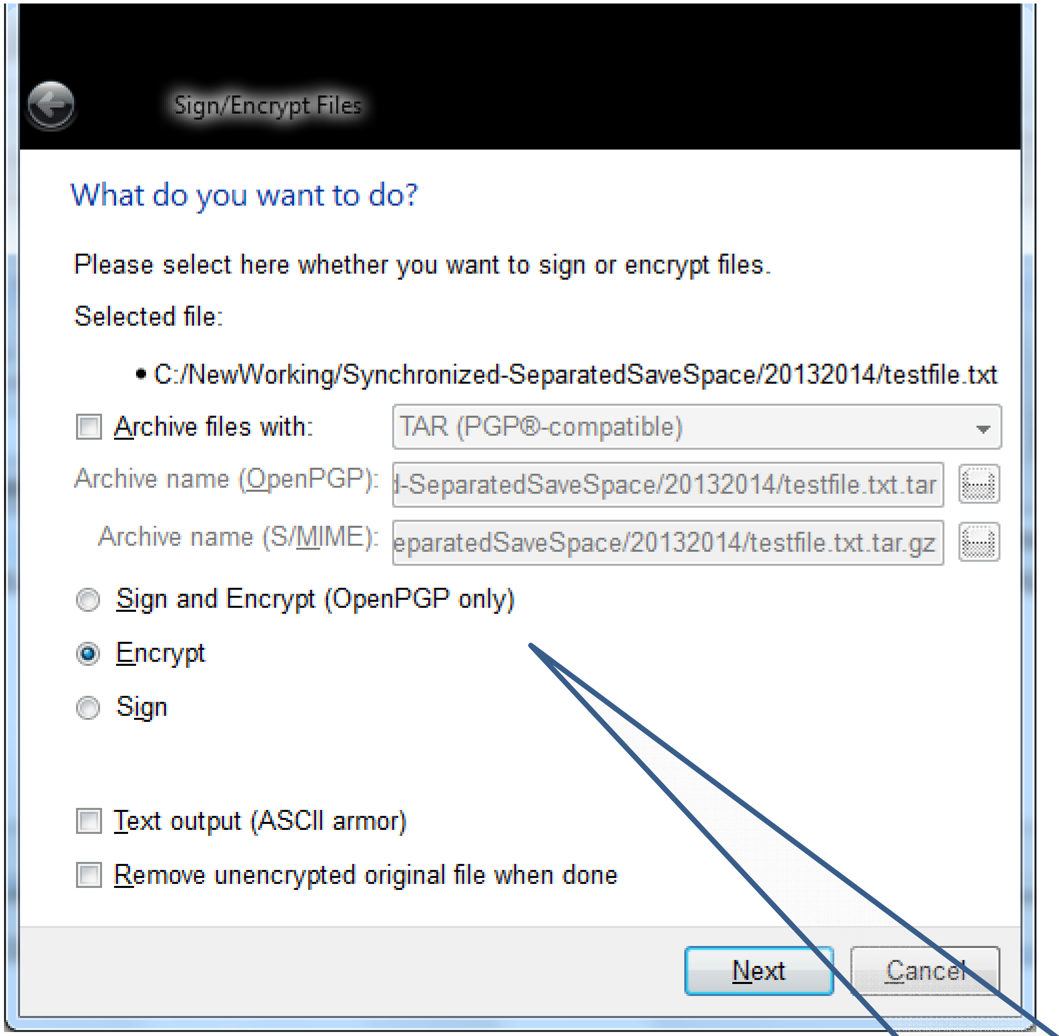
«testfile.txt» [New file] 3 lines, 54 characters  i  –100%–  00003  028

This is the file to be digitally signed (testfile.txt)


Kleopatra
File
View
Certificates
Tools
Settings
Window
Help
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E
Decrypt/Verify Files...
Sign/Encrypt Files...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Lookup Certificates on Server
My Certificates
cates

| l | Valid From | Valid Until | Details | Key-ID |
|---|---|---|---|---|
| lu | 2013-05-08 | | OpenPGP | 6ADC6FEA |

Click “File -> Sign/Encrypt Files …”



What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- C:/NewWorking/Synchronized-SeparatedSaveSpace/20132014/testfile.txt

□ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): l-SeparatedSaveSpace/20132014/testfile.txt.tar

Archive name (S/MIME): eparatedSaveSpace/20132014/testfile.txt.tar.gz

○ Sign and Encrypt (OpenPGP only)

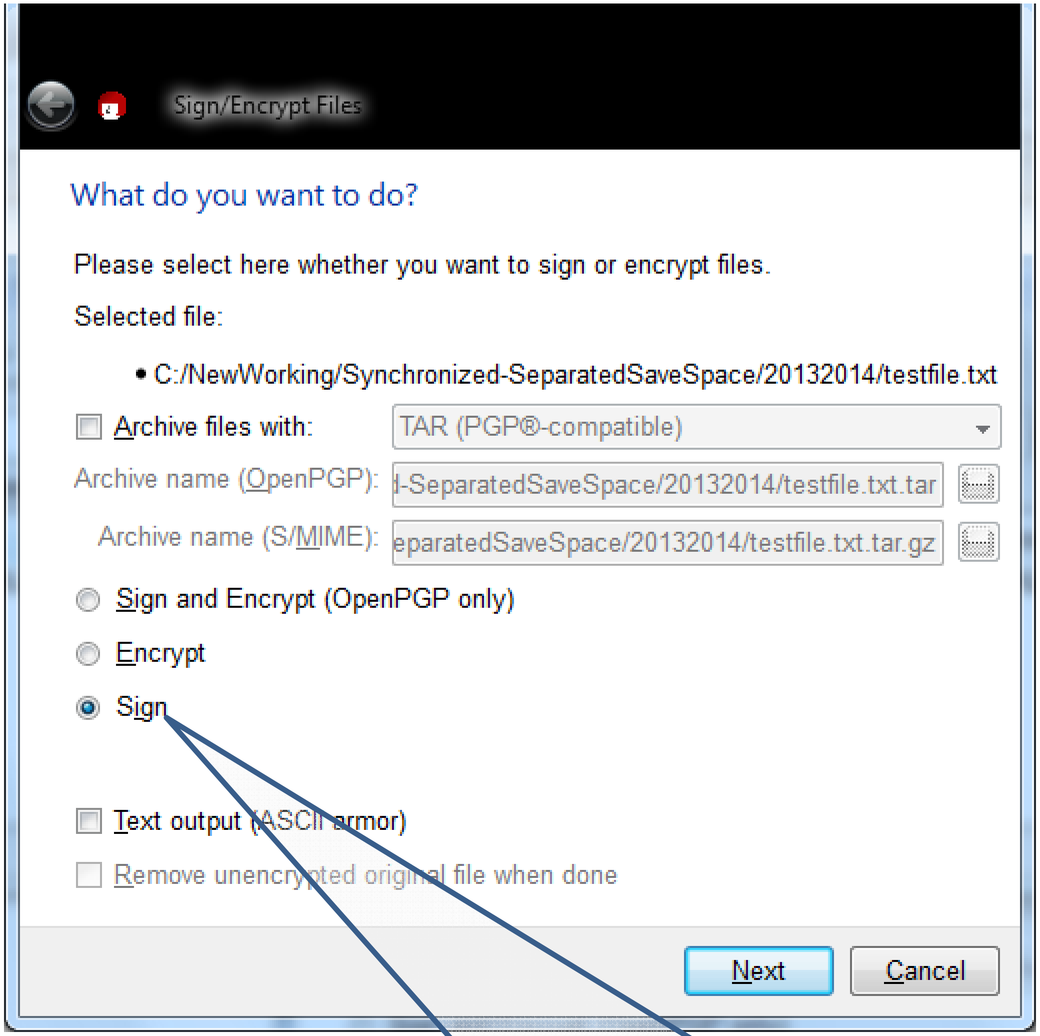
● Encrypt

○ Sign

□ Text output (ASCII armor)

□ Remove unencrypted original file when done

You have three choices



Sign/Encrypt Files

What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- C:/NewWorking/Synchronized-SeparatedSaveSpace/20132014/testfile.txt

□ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): l-SeparatedSaveSpace/20132014/testfile.txt.tar

Archive name (S/MIME): eparatedSaveSpace/20132014/testfile.txt.tar.gz

○ Sign and Encrypt (OpenPGP only)

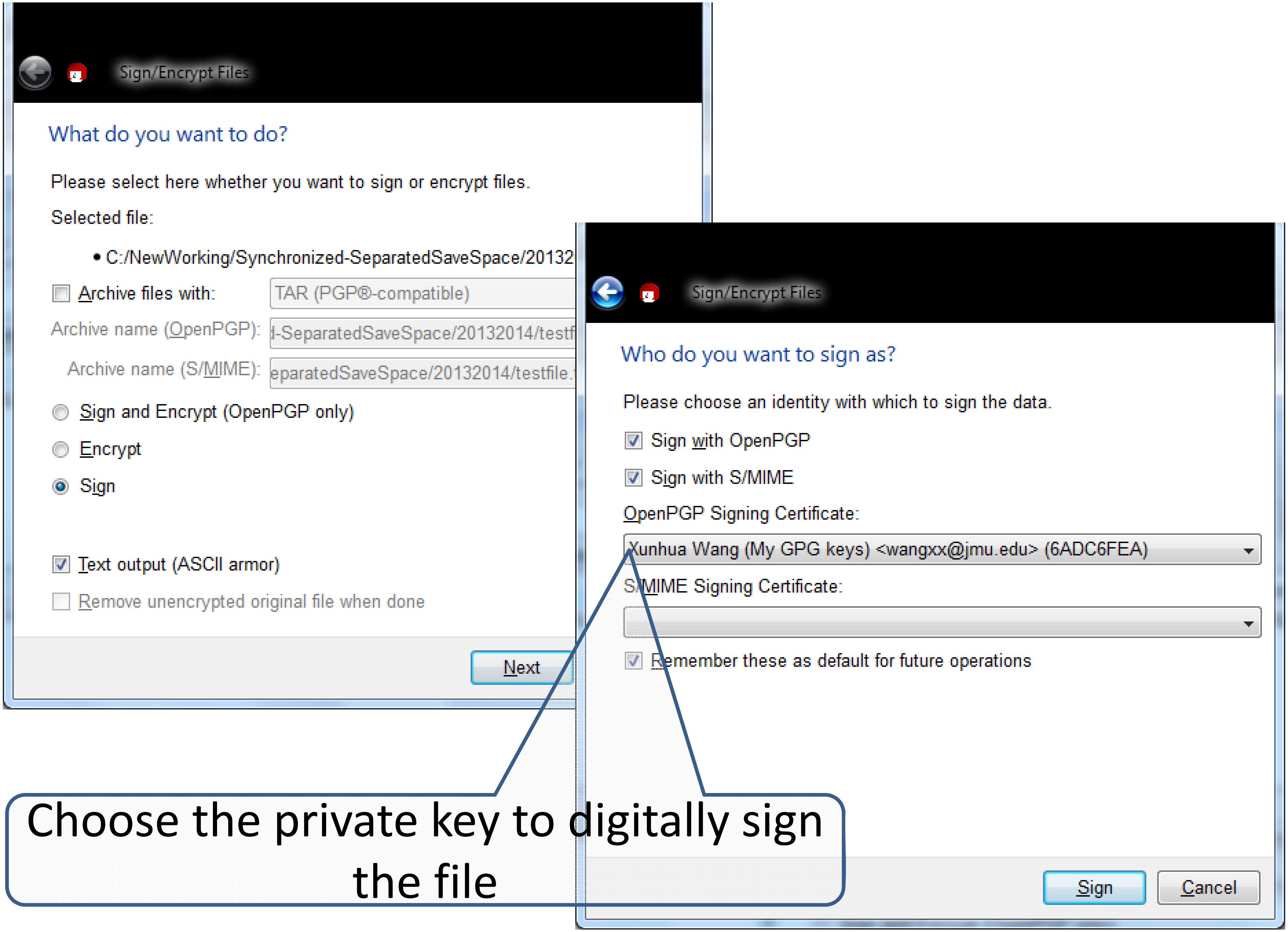
○ Encrypt

● Sign

□ Text output (ASCII armor)

□ Remove unencrypted original file when done

I want to digitally sign the file this time



Sign/Encrypt Files

## What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

- C:/NewWorking/Synchronized-SeparatedSaveSpace/20132

□ Archive files with: TAR (PGP®-compatible)

Archive name (OpenPGP): l-SeparatedSaveSpace/20132014/testf

Archive name (S/MIME): eparatedSaveSpace/20132014/testfile.

○ Sign and Encrypt (OpenPGP only)

○ Encrypt

● Sign

☑ Text output (ASCII armor)

□ Remove unencrypted original file when done

Sign/Encrypt Files

## Who do you want to sign as?

Please choose an identity with which to sign the data.

☑ Sign with OpenPGP

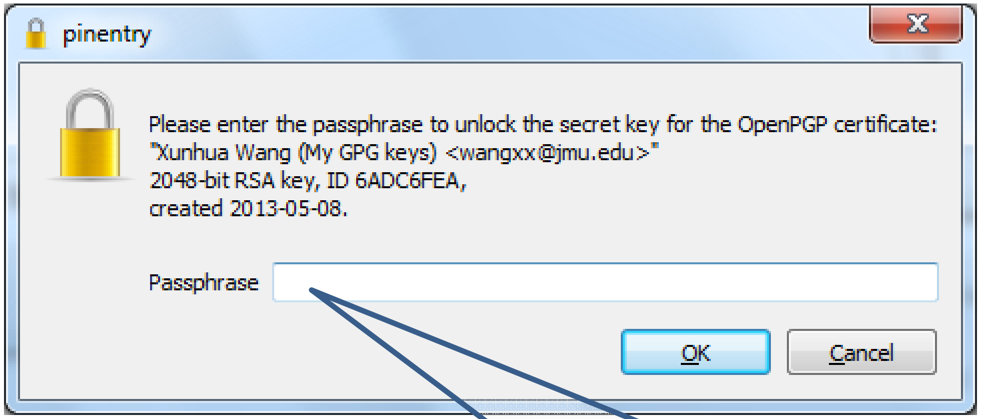
☑ Sign with S/MIME

OpenPGP Signing Certificate: Xunhua Wang (My GPG keys) <wangxx@jmu.edu> (6ADC6FEA)

S/MIME Signing Certificate:

☑ Remember these as default for future operations

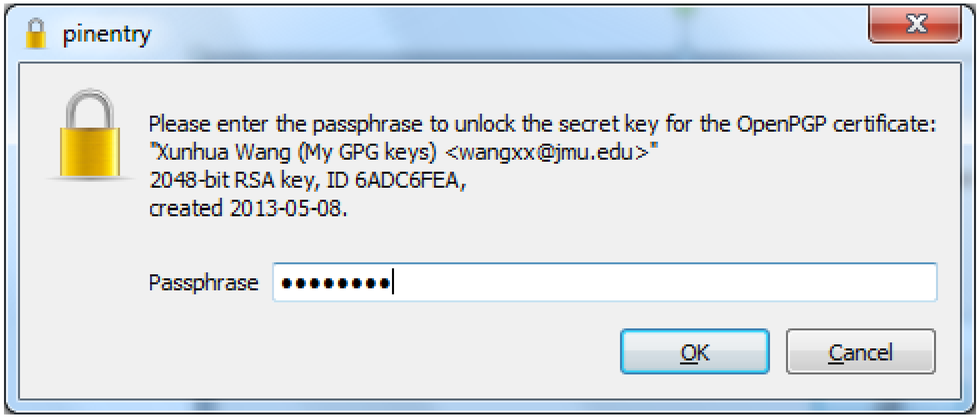
Choose the private key to digitally sign the file



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Xunhua Wang (My GPG keys) <wangxx@jmu.edu>"
2048-bit RSA key, ID 6ADC6FEA,
created 2013-05-08.

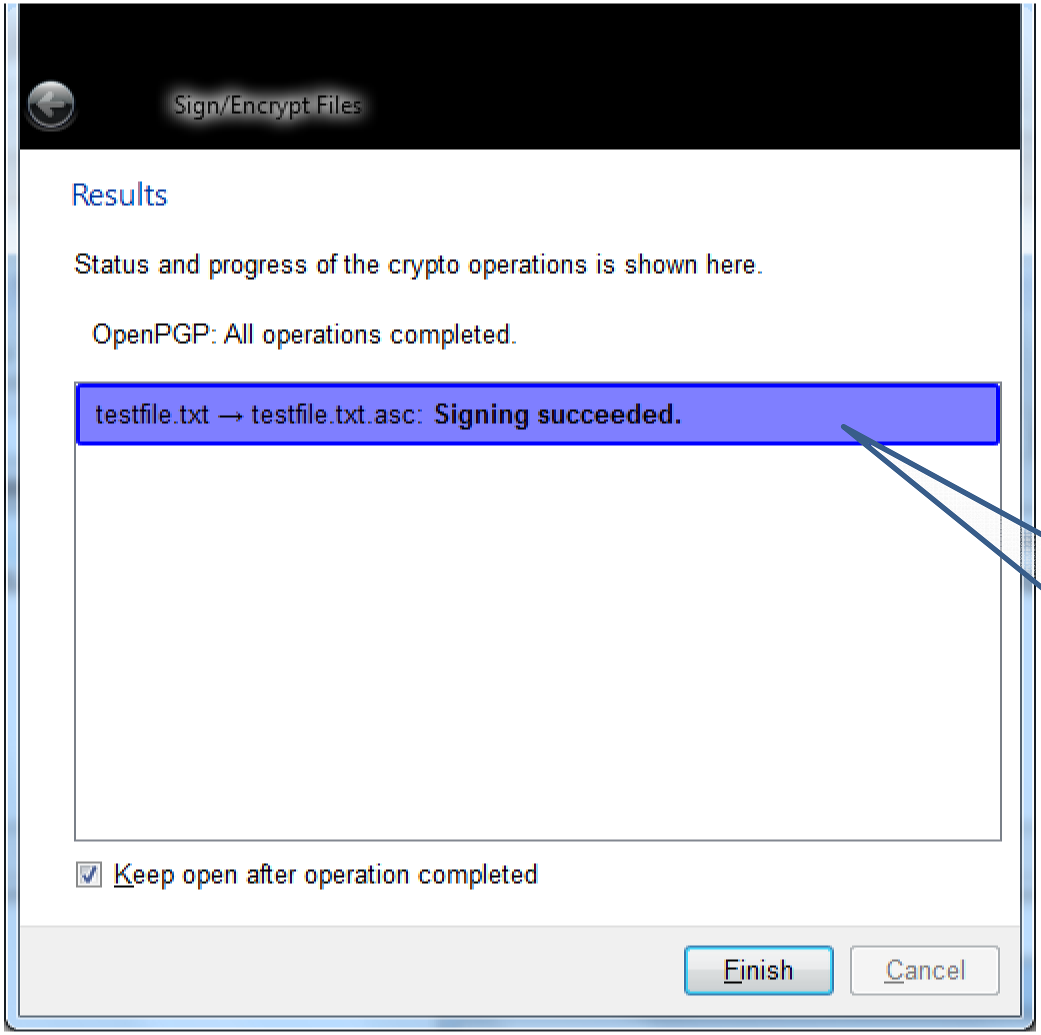
Passphrase

My private key is protected by a password



Please enter the passphrase to unlock the secret key for the OpenPGP certificate:
"Xunhua Wang (My GPG keys) <wangxx@jmu.edu>"
2048-bit RSA key, ID 6ADC6FEA,
created 2013-05-08.

Passphrase •••••••••



Results

Status and progress of the crypto operations is shown here.

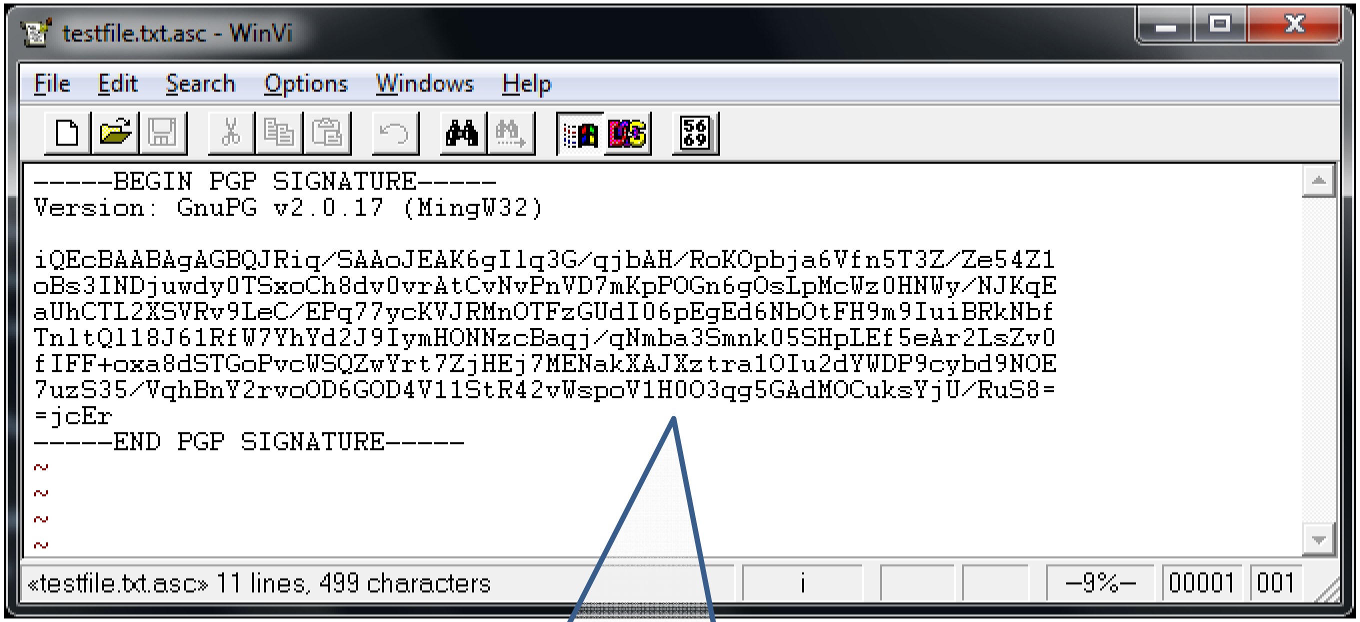
OpenPGP: All operations completed.

testfile.txt → testfile.txt.asc: **Signing succeeded.**

☑ Keep open after operation completed

Everything is cool

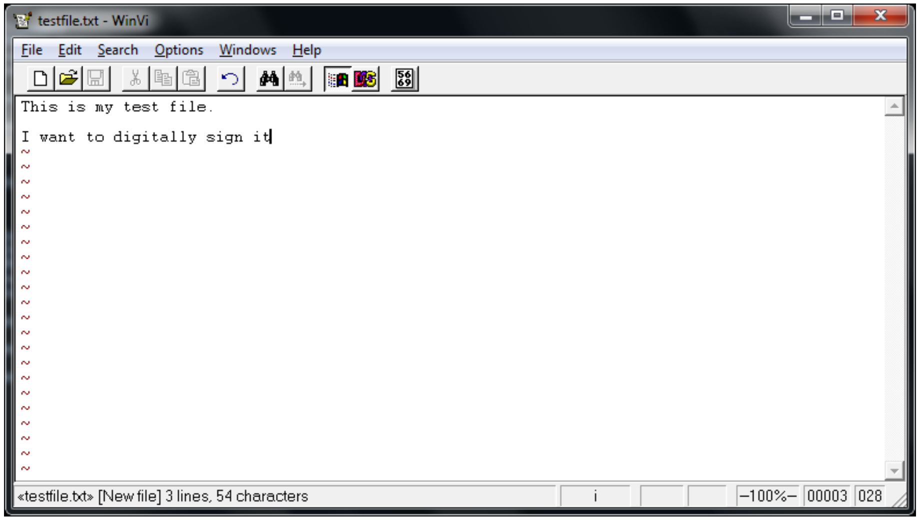
So, where is the digital signature for my file?



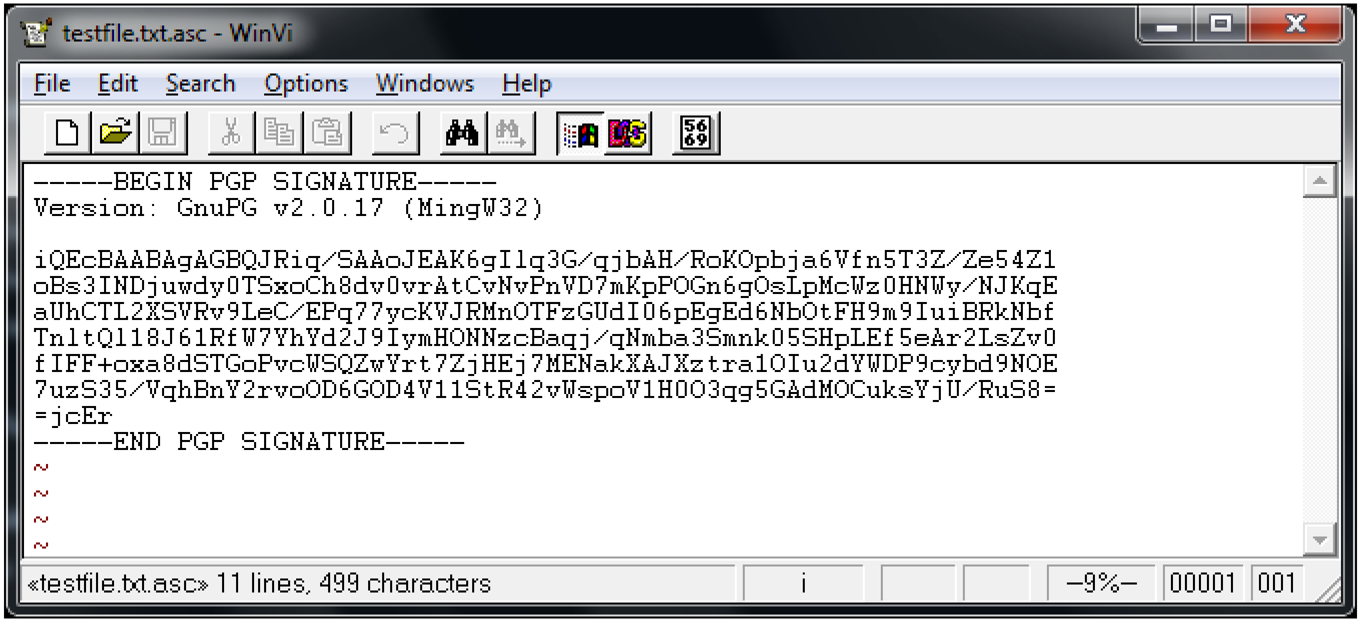
```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.17 (MingW32)

iQEcBAABAgAGBQJRiq/SAAoJEAK6gIlq3G/qjbAH/RoKOpbja6Vfn5T3Z/Ze54Z1
oBs3INDjuwdy0TSxoCh8dv0vrAtCvNvPnVD7mKpPOGn6gOsLpMcWz0HNWy/NJKqE
aUhCTL2XSVRv9LeC/EPq77ycKVJRMnOTFzGUdI06pEgEd6NbOtFH9m9IuiBRkNbf
TnltQl18J61RfW7YhYd2J9IymHONNzcBaqj/qNmba3Smnk05SHpLEf5eAr2LsZv0
fIFF+oxa8dSTGoPvcWSQZwYrt7ZjHEj7MENakXAJXztra1OIu2dYWDP9cybd9NOE
7uzS35/VqhBnY2rvoOD6GOD4V11StR42vWspoV1HOO3qg5GAdMOCuksYjU/RuS8=
=jcEr
-----END PGP SIGNATURE-----
~
~
~
~
```

«testfile.txt.asc» 11 lines, 499 characters

My file is testfile.txt and the signature file is called testfile.txt.asc

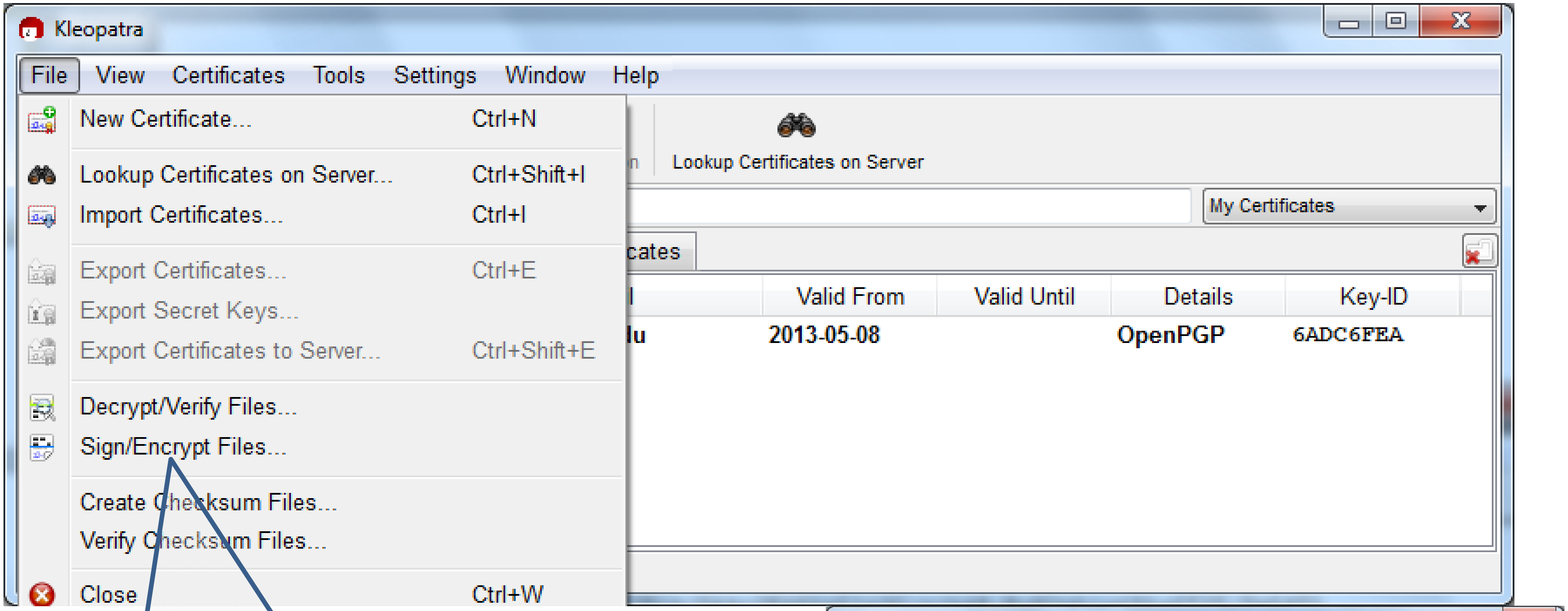

testfile.txt - WinVi
File Edit Search Options Windows Help
«testfile.txt» [New file] 3 lines, 54 characters
i
–100%–
00003
028

```
This is my test file.

I want to digitally sign it
```


testfile.txt.asc - WinVi
File Edit Search Options Windows Help
«testfile.txt.asc» 11 lines, 499 characters
i
–9%–
00001
001

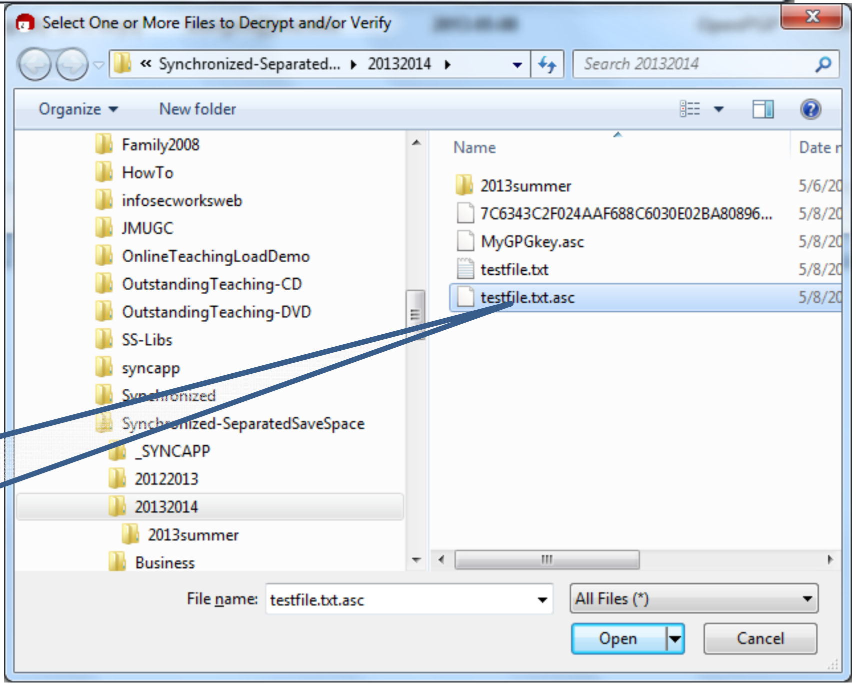
```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.17 (MingW32)

iQEcBAABAgAGBQJRiq/SAAoJEAK6gIlq3G/qjbAH/RoKOpbja6Vfn5T3Z/Ze54Z1
oBs3INDjuwdy0TSxoCh8dv0vrAtCvNvPnVD7mKpPOGn6gOsLpMcWz0HNWy/NJKqE
aUhCTL2XSVRv9LeC/EPq77ycKVJRMnOTFzGUdI06pEgEd6NbOtFH9m9IuiBRkNbf
TnltQl18J61RfW7YhYd2J9IymHONNzcBaqj/qNmba3Smnk05SHpLEf5eAr2LsZv0
fIFF+oxa8dSTGoPvcWSQZwYrt7ZjHEj7MENakXAJXztra1OIu2dYWDP9cybd9NOE
7uzS35/VqhBnY2rvoOD6GOD4V11StR42vWspoV1HOO3qg5GAdMOCuksYjU/RuS8=
=jcEr
-----END PGP SIGNATURE-----
```

Next, I email both my file **<u>and</u>** the signature file to Bob (my classmate)



Kleopatra
File
View
Certificates
Tools
Settings
Window
Help
New Certificate... Ctrl+N
Lookup Certificates on Server... Ctrl+Shift+I
Import Certificates... Ctrl+I
Export Certificates... Ctrl+E
Export Secret Keys...
Export Certificates to Server... Ctrl+Shift+E
Decrypt/Verify Files...
Sign/Encrypt Files...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Lookup Certificates on Server
My Certificates

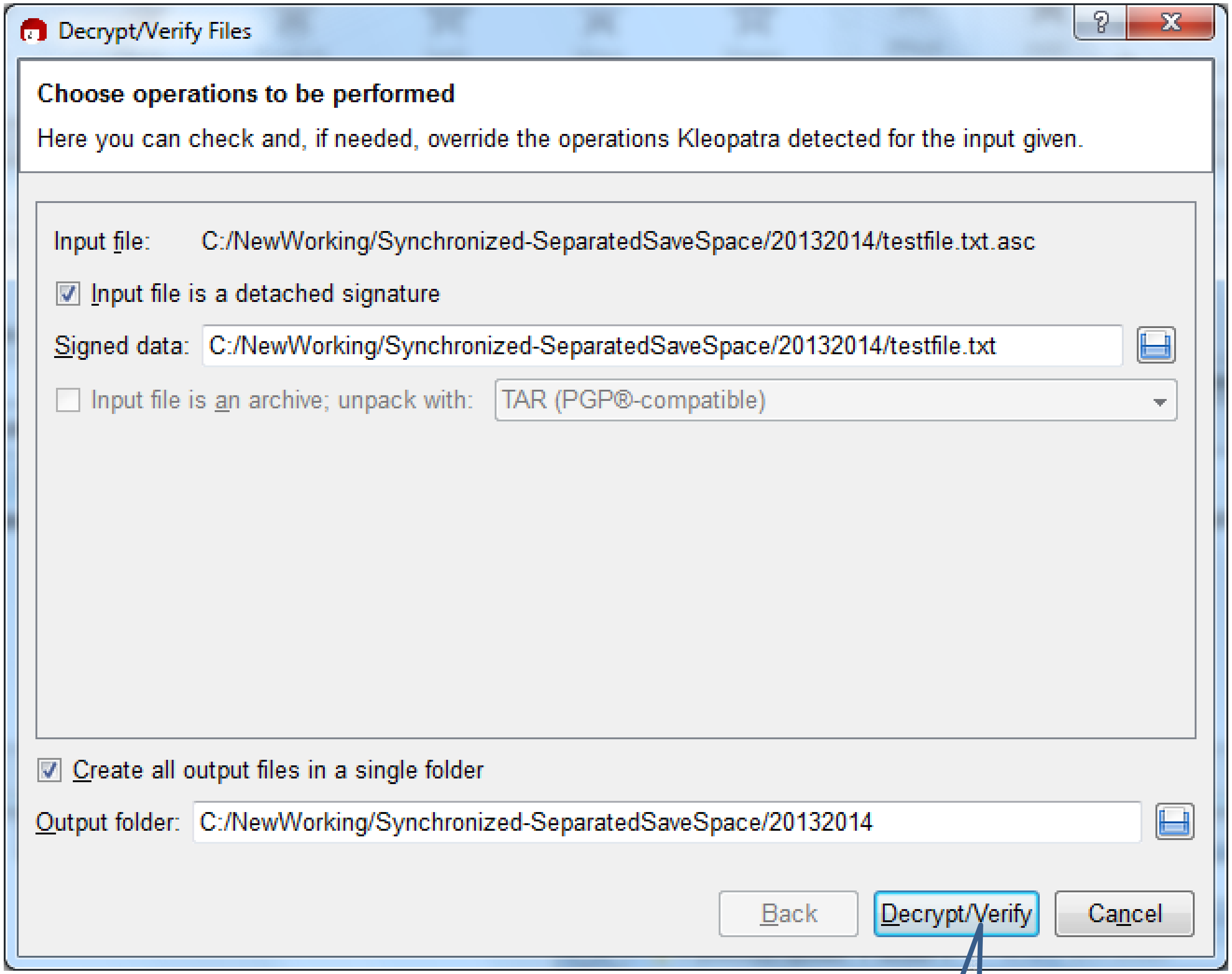
| Valid From | Valid Until | Details | Key-ID |
|---|---|---|---|
| 2013-05-08 | | OpenPGP | 6ADC6FEA |



File name: testfile.txt.asc

**Bob**: Click “File -> Decrypt/Verify Files ...”

**Bob** selects the signature file received from me



Decrypt/Verify Files

**Choose operations to be performed**

Here you can check and, if needed, override the operations Kleopatra detected for the input given.

Input file: C:/NewWorking/Synchronized-SeparatedSaveSpace/20132014/testfile.txt.asc

☑ Input file is a detached signature

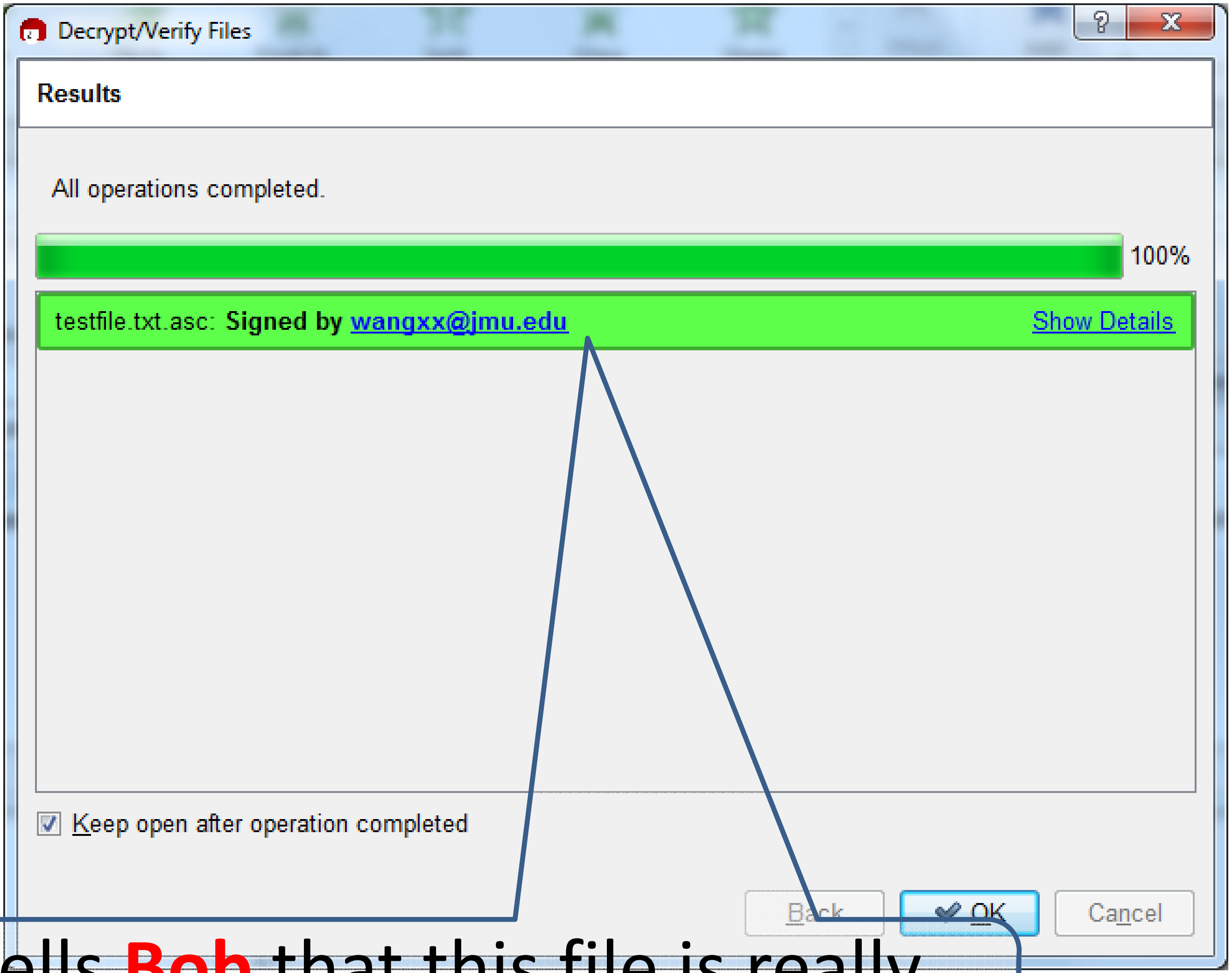
Signed data: C:/NewWorking/Synchronized-SeparatedSaveSpace/20132014/testfile.txt

☐ Input file is an archive; unpack with: TAR (PGP®-compatible)

☑ Create all output files in a single folder

Output folder: C:/NewWorking/Synchronized-SeparatedSaveSpace/20132014

Bob:



Decrypt/Verify Files

**Results**

All operations completed.

100%

testfile.txt.asc: **Signed by wangxx@jmu.edu**

☑ Keep open after operation completed

It tells **Bob** that this file is really from me, not from an attacker

# Exercise #2

❸Create a text file *your_first_name-last_name-gpg4win.txt* and digitally sign it

❹Email *your_first_name-last_name-gpg4win.txt* **and** the digital signature file to your classmate

❺After receiving the files from your classmate, try to digitally verify them

# What if I want to digitally sign

- An email?
  - Not a file

- GnuPG for Outlook (GpgOL)
  - Use with Microsoft Outlook mail client

# Summary

- Practice
  - Truecrypt
  - GPG

# One More Note

- You can encrypt
  - a MS Word file with a password
    - MS Word allows you to do this
  - a MS Excel file with a password
    - MS Excel allows you to do this
  - a PDF file with a password
    - Adobe Acrobat allows you to do this

# GPG on Unix/Linux (1/5)

- gpg --gen-key
  - User ID: real name, email address, comment
  - Passphrase for your private key
  - /home/user/.gnupg/trustdb.gpg
- Revocation certificate
  - gpg –a --output wangxx@jmu.edu.asc.revoke --gen-revoke wangxx@jmu.edu
    - Reason: 0
- Publicizing your key
  - gpg ---output pubkey.wangxx@jmu.edu.gpg --export wangxx
  - gpg ---output pubkey.wangxx@jmu.edu.gpg.asc --armor --export wangxx
  - gpg --keyserver subkeys.gpg.net --send-keys wangxx@jmu.edu

# On Linux

- GPG is also available on Linux

# GPG on Unix/Linux (2/5)

- keyserver x-hkp://subkeys.pgp.net

- Add keys to your keyring (public vs. private)
  - gpg --recv-keys E68C49BC
  - gpg --list-keys
  - gpg --list-secret-keys
  - gpg --list-keys wangxx@jmu.edu
  - gpg --import wang.asc

# GPG on Unix/Linux (3/5)

- Signing a key
  - gpg --fingerprint wangxx@jmu.edu
  - gpg --sign-key E2F41133
- Viewing key signatures
  - gpg --list-sigs E2F41133
- Export
  - gpg --output wangxx.asc --armor --export E2F41133
- Pushing signatures to keyservers
  - gpg --send-keys E2F41133
- Updating keys
  - gpg --refresh-keys

# GPG on Unix/Linux (4/5)

- Deleting keys
  - gpg --delete-keys E2F41133

- gpg --update-trustdb

# GPG on Unix/Linux (5/5)

- To digitally sign a file
  - gpg –s filename
- To verify a digital signature
  - gpg --verify filenameOfSignature

- Encrypt data
  - gpg –e filename
- Decrypt data
  - gpg --decrypt msg.asc