Cryptography: Practice

2015 JMU Cyber Defense Boot Camp

Prerequisites

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

To do what?

- Protect files in a virtual container or on your USB drive
  - Like a bank vault

- To encrypt and digitally sign an email

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
  - ❶Truecrypt
  - ❷GPG
  - ❸BitLocker

We may not have enough time to finish all three practices.
You can do ❸ afterwards

Road Map

- Practice
  - ❶Truecrypt
  - ❷GPG
  - ❸BitLocker

TrueCrypt

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

Step 1

- Download and install
  - https://truecrypt.ch/downloads/

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

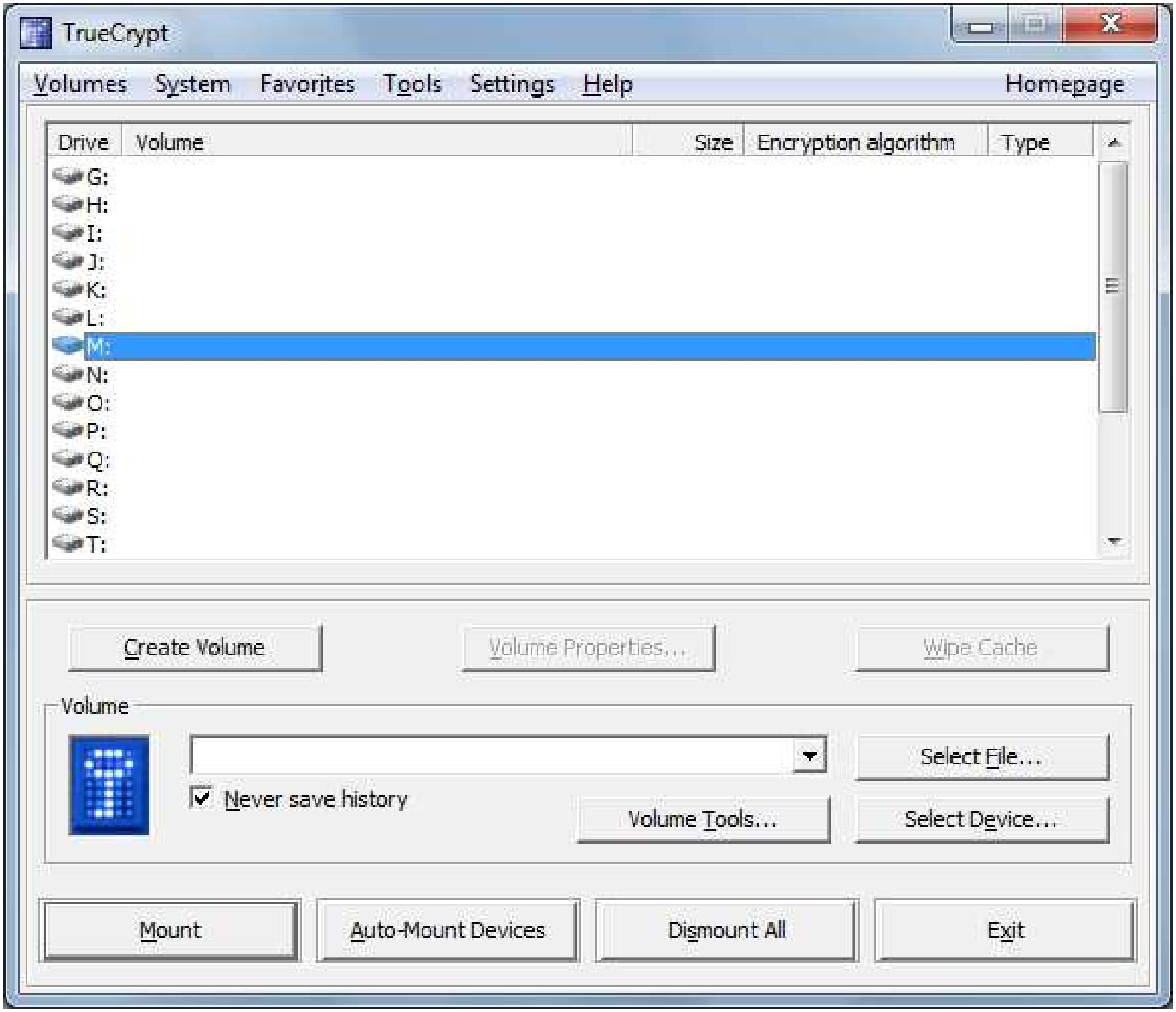
Step 2: Run TrueCrypt

- Start > All Programs > TrueCrypt > TrueCrypt

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

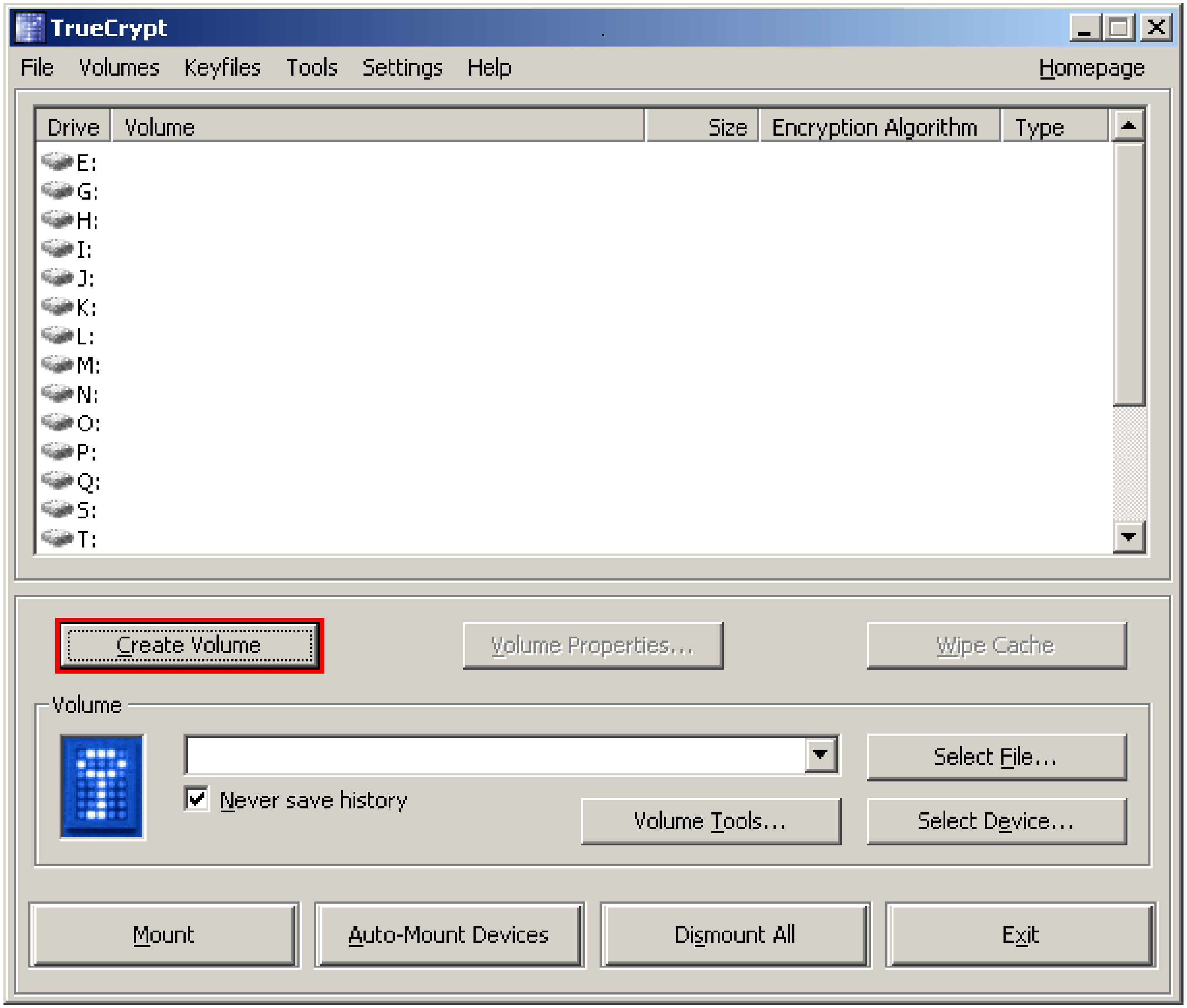
Step 2

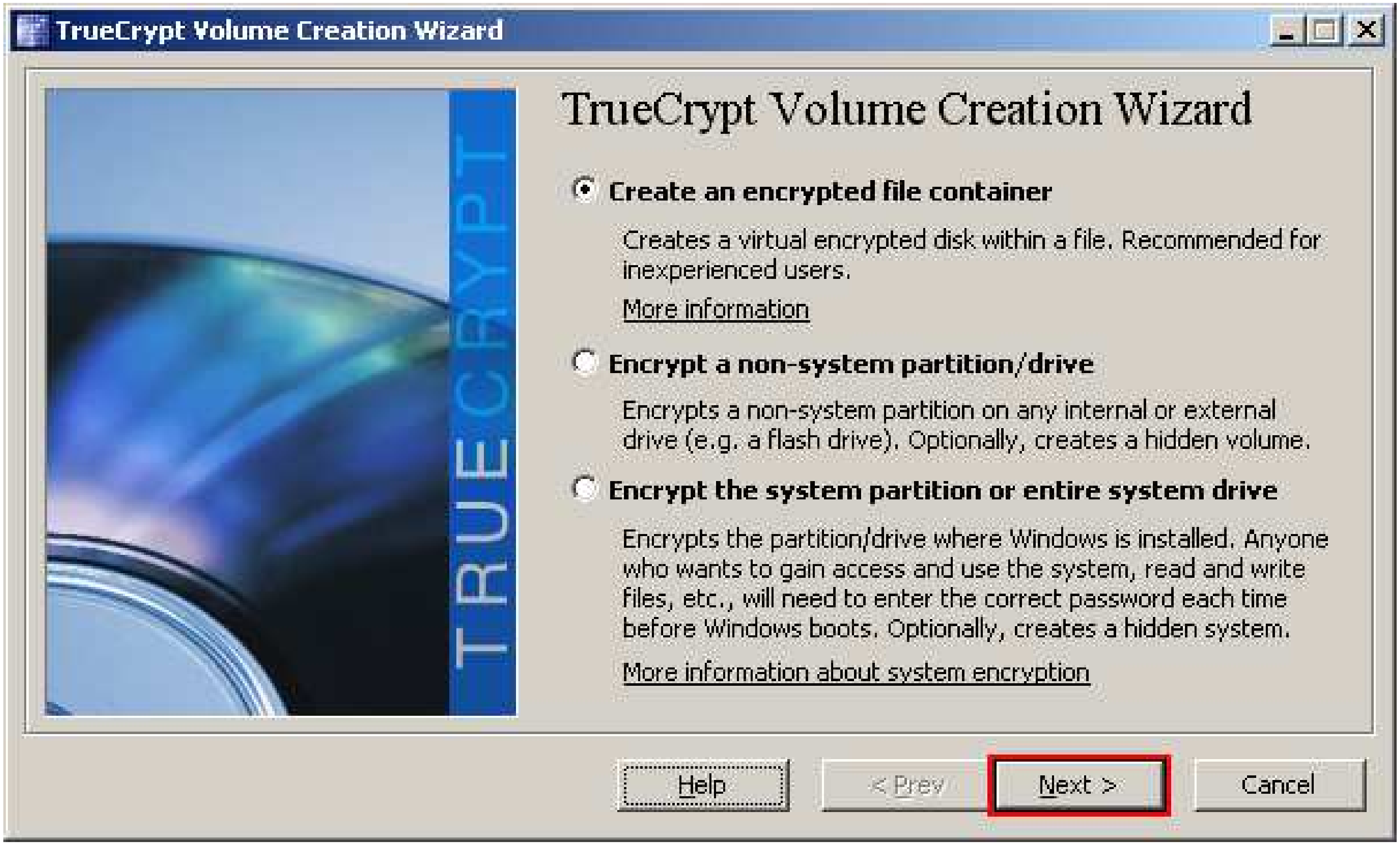
- Create a virtual encrypted disk (called file container)
  - Then put all of your critical files there



☑ Never save history

CREDITS: some of these screen snapshots are from https://download.truecrypt.ch/documentation/TrueCrypt%20User%20Guide.pdf





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**

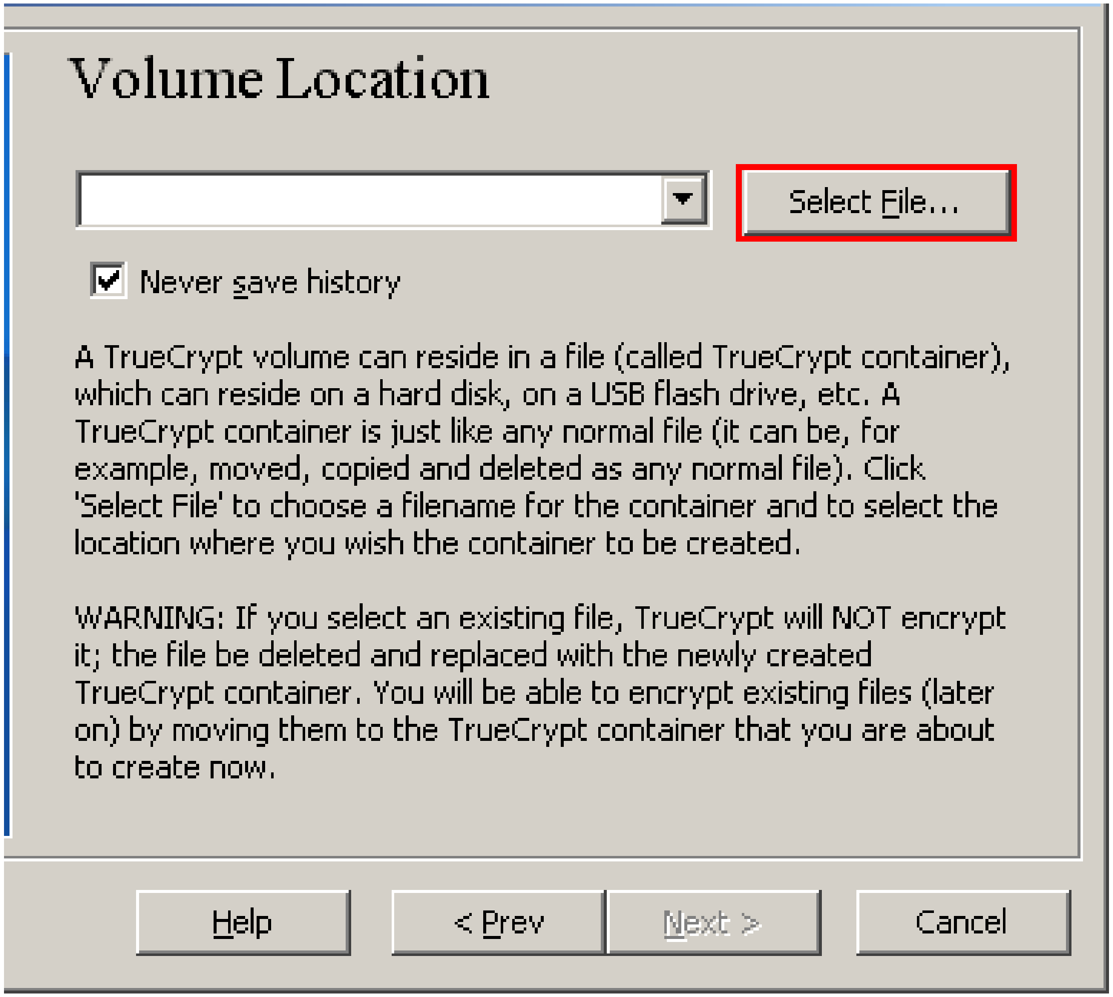
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **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

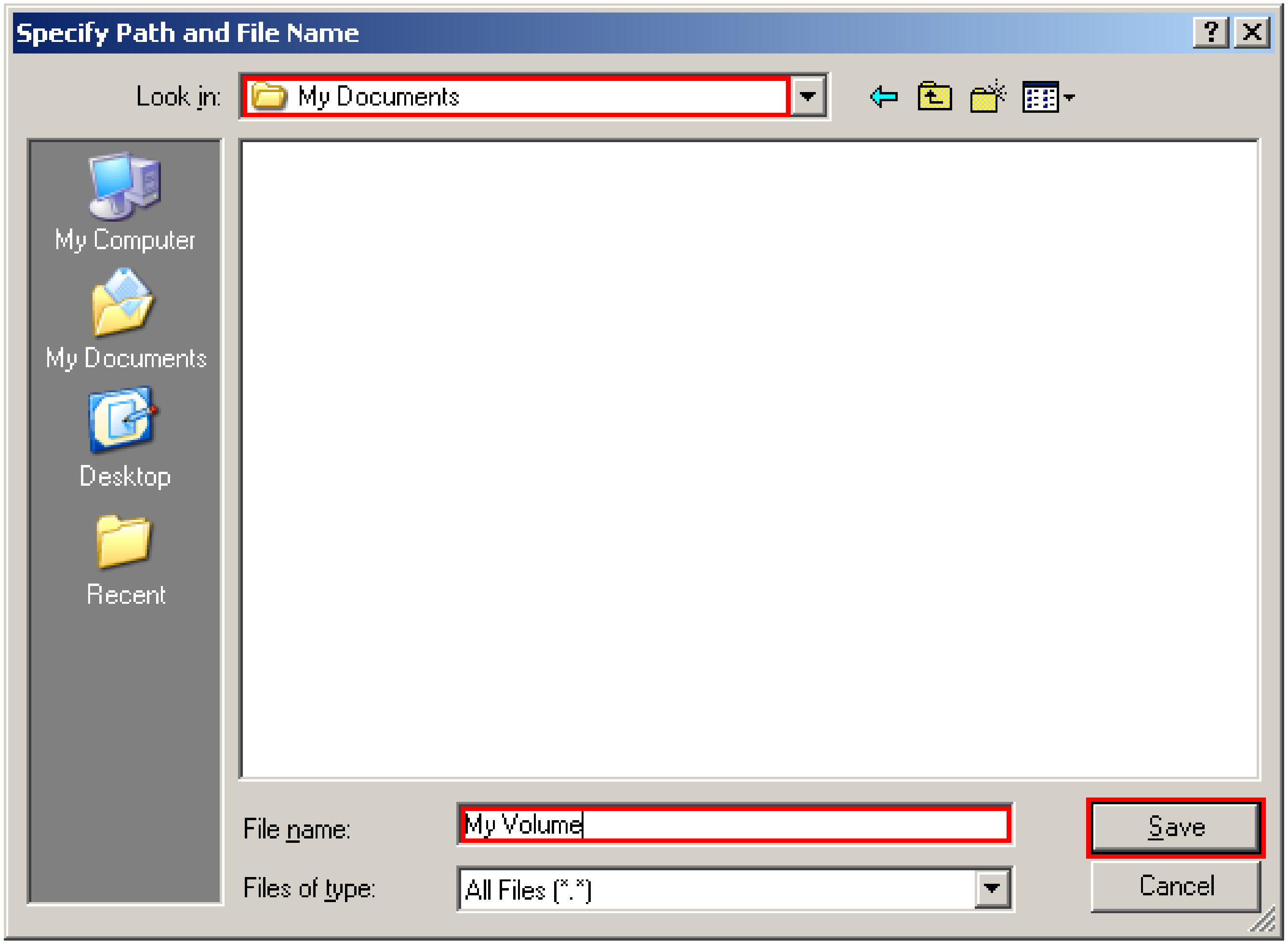
The Location of the Virtual Encrypted Disk



☑ Never save history

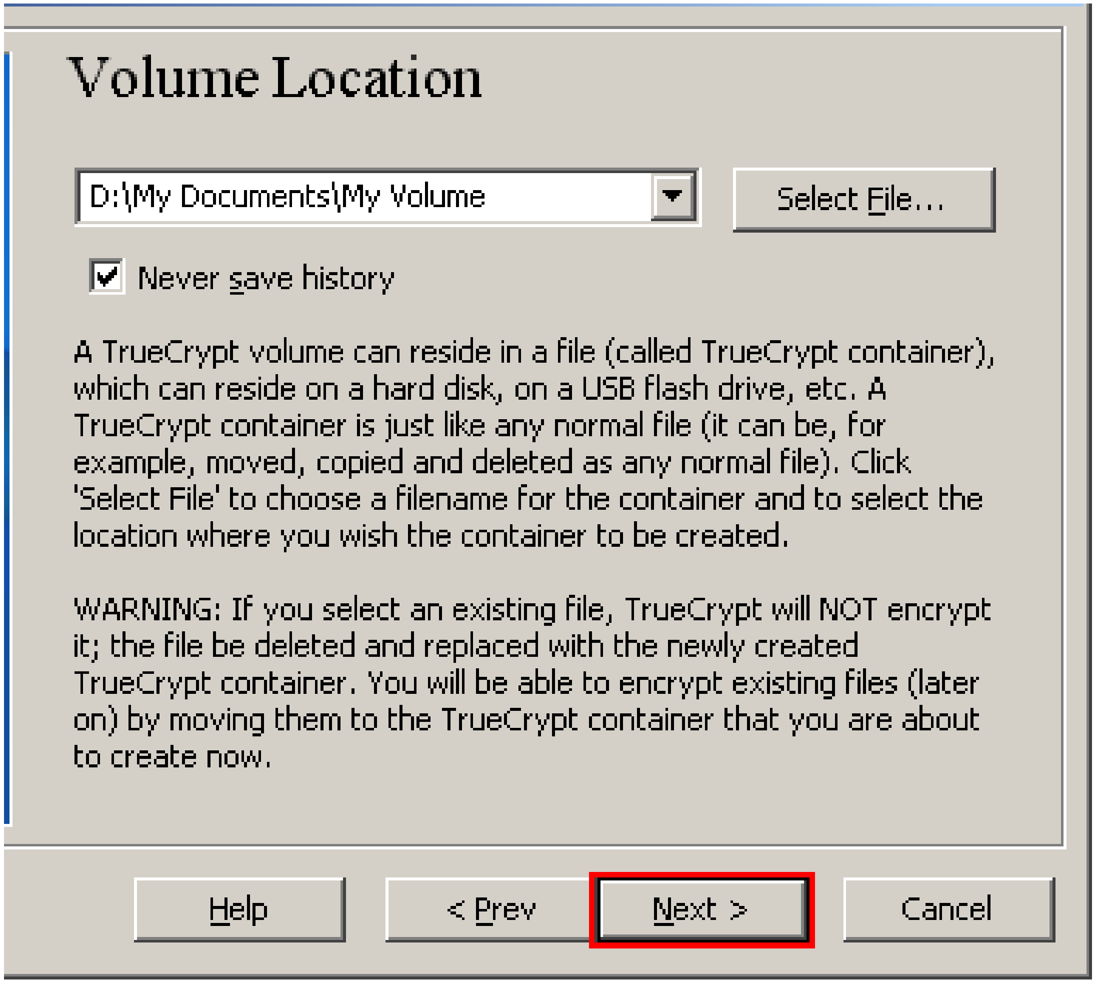
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the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



File name: My Volume

Files of type: All Files (*.*)



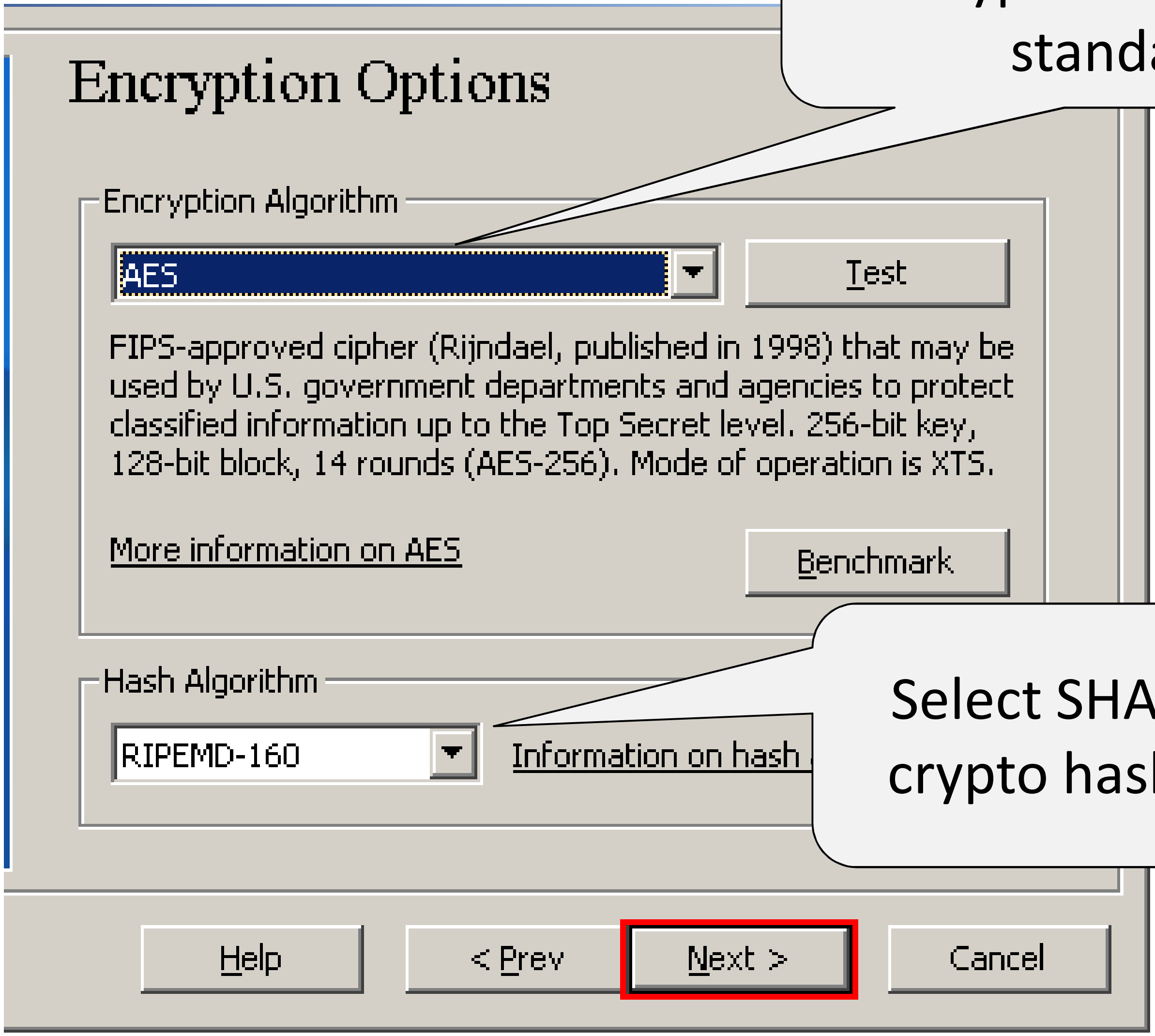
Volume Location

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

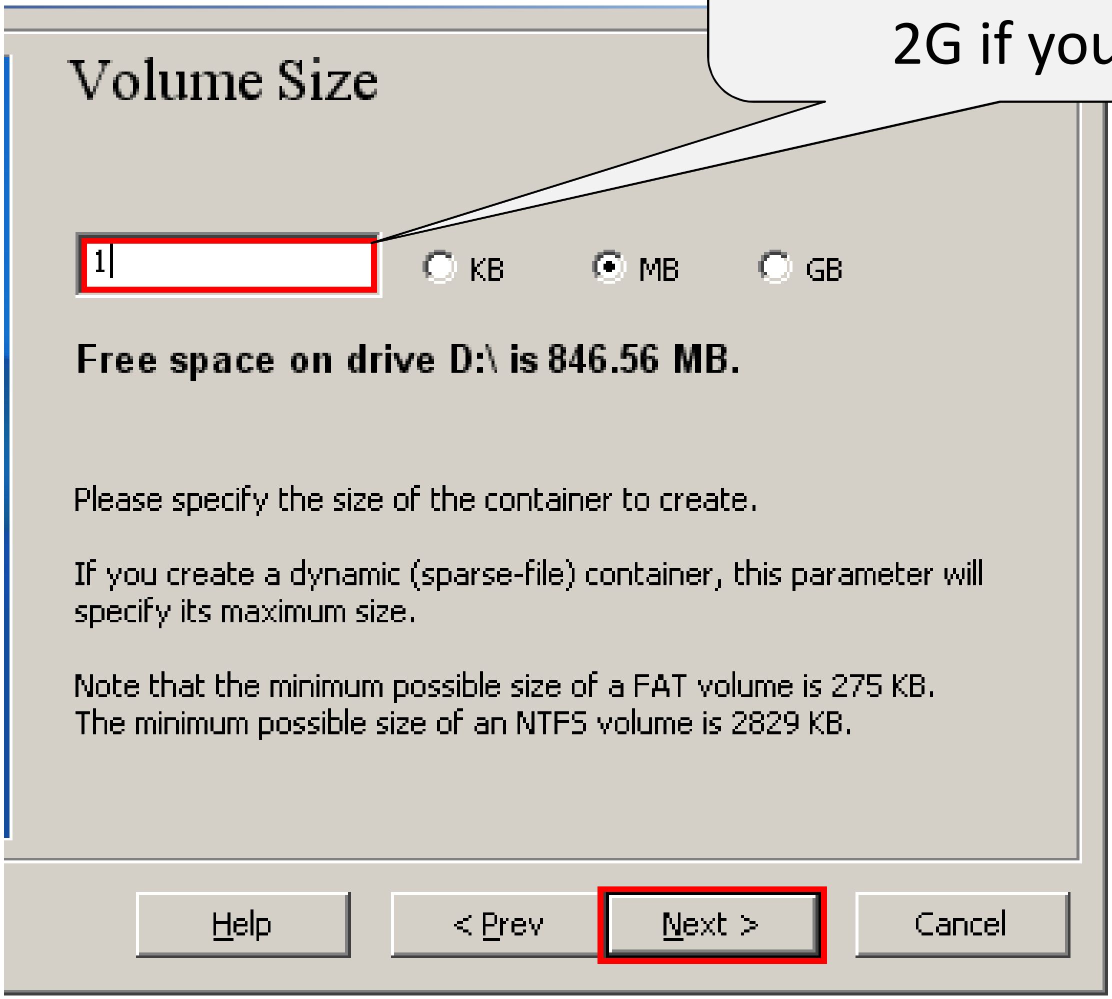
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

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

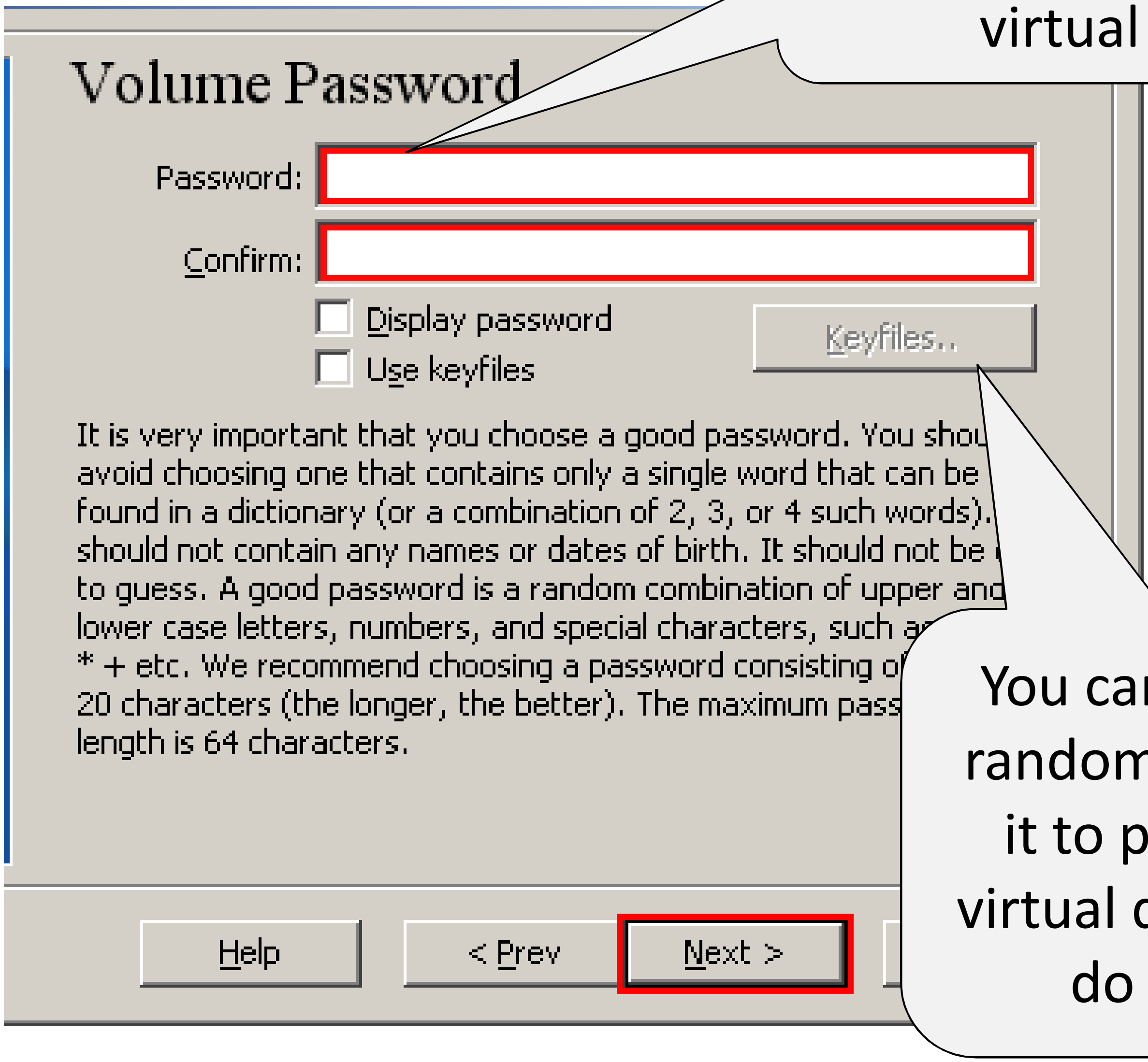
Free space on drive D:\ is 846.56 MB.

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

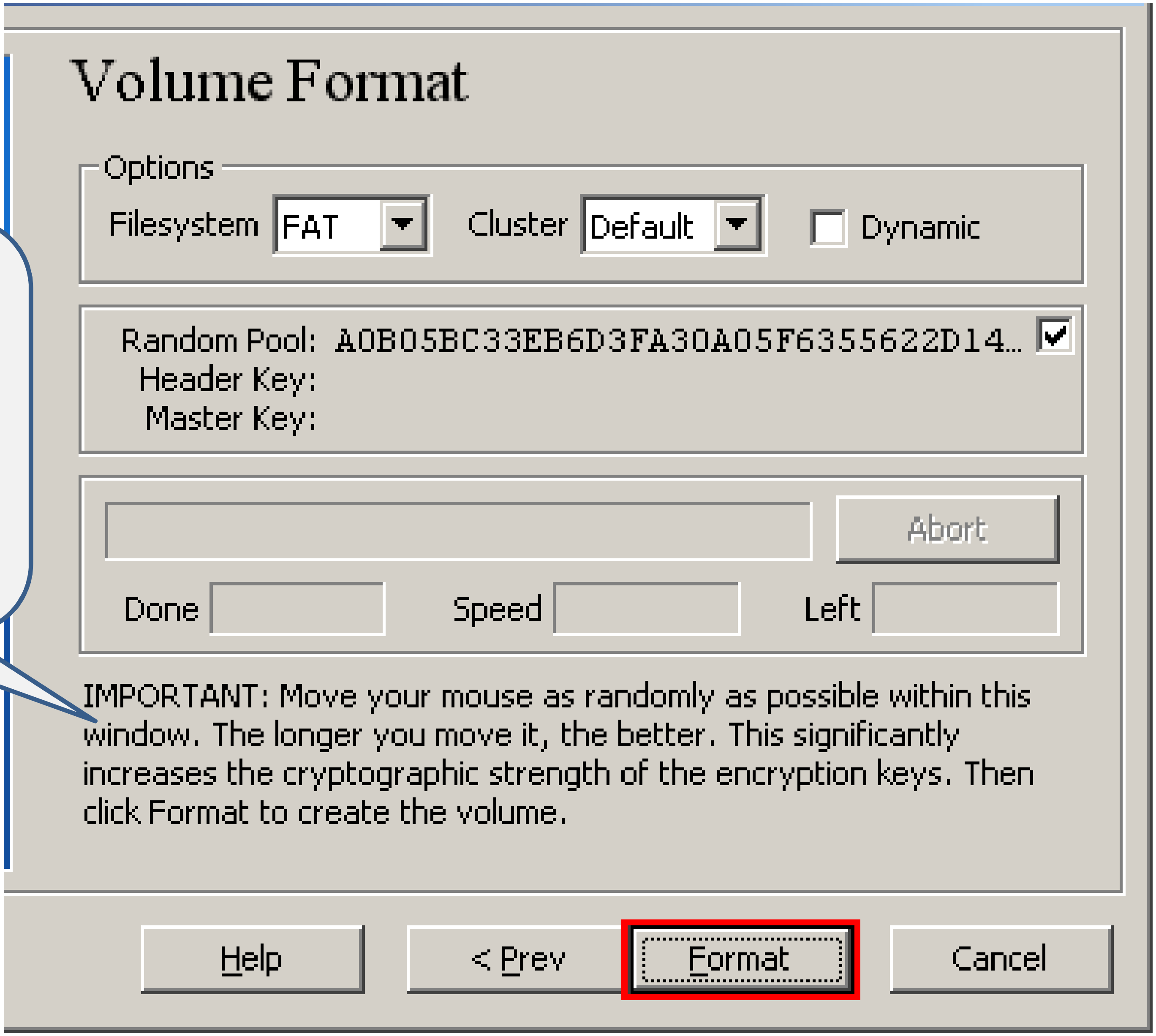
□ Use keyfiles

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

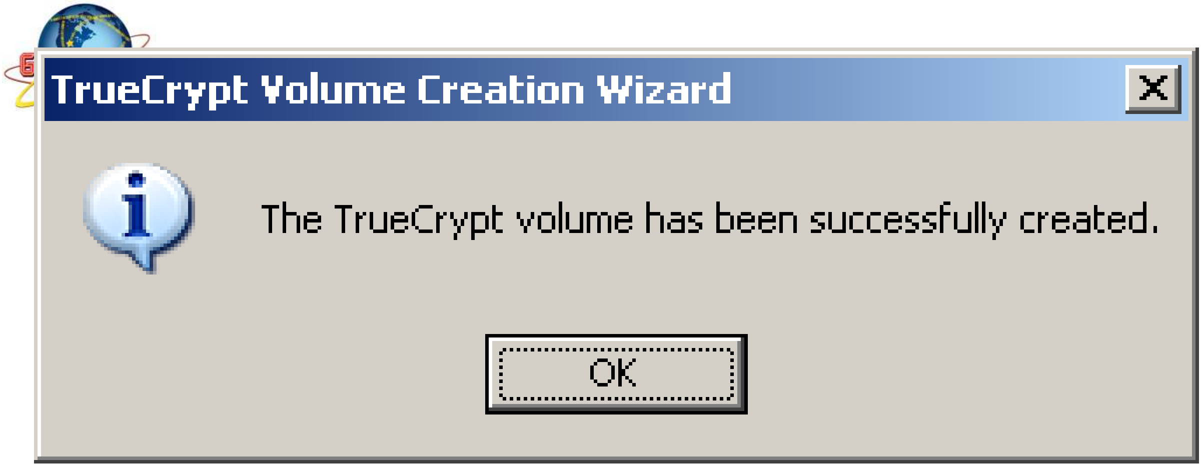
Options

Filesystem FAT Cluster Default □ Dynamic

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

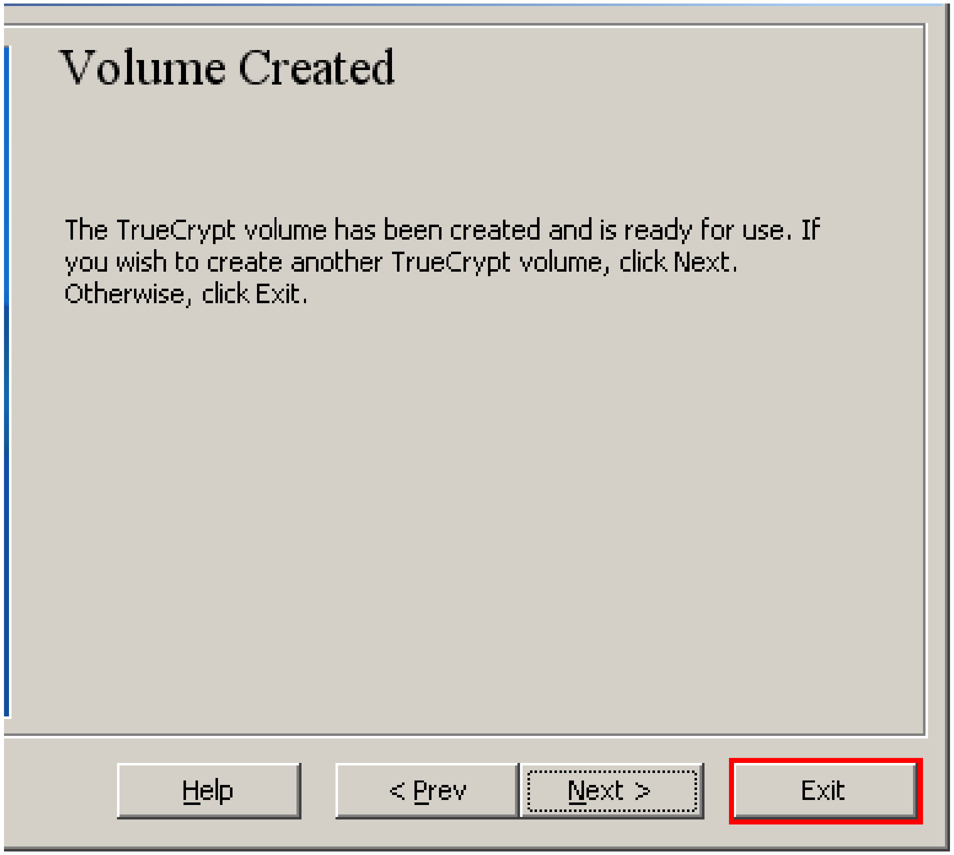
Done Speed Left

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.



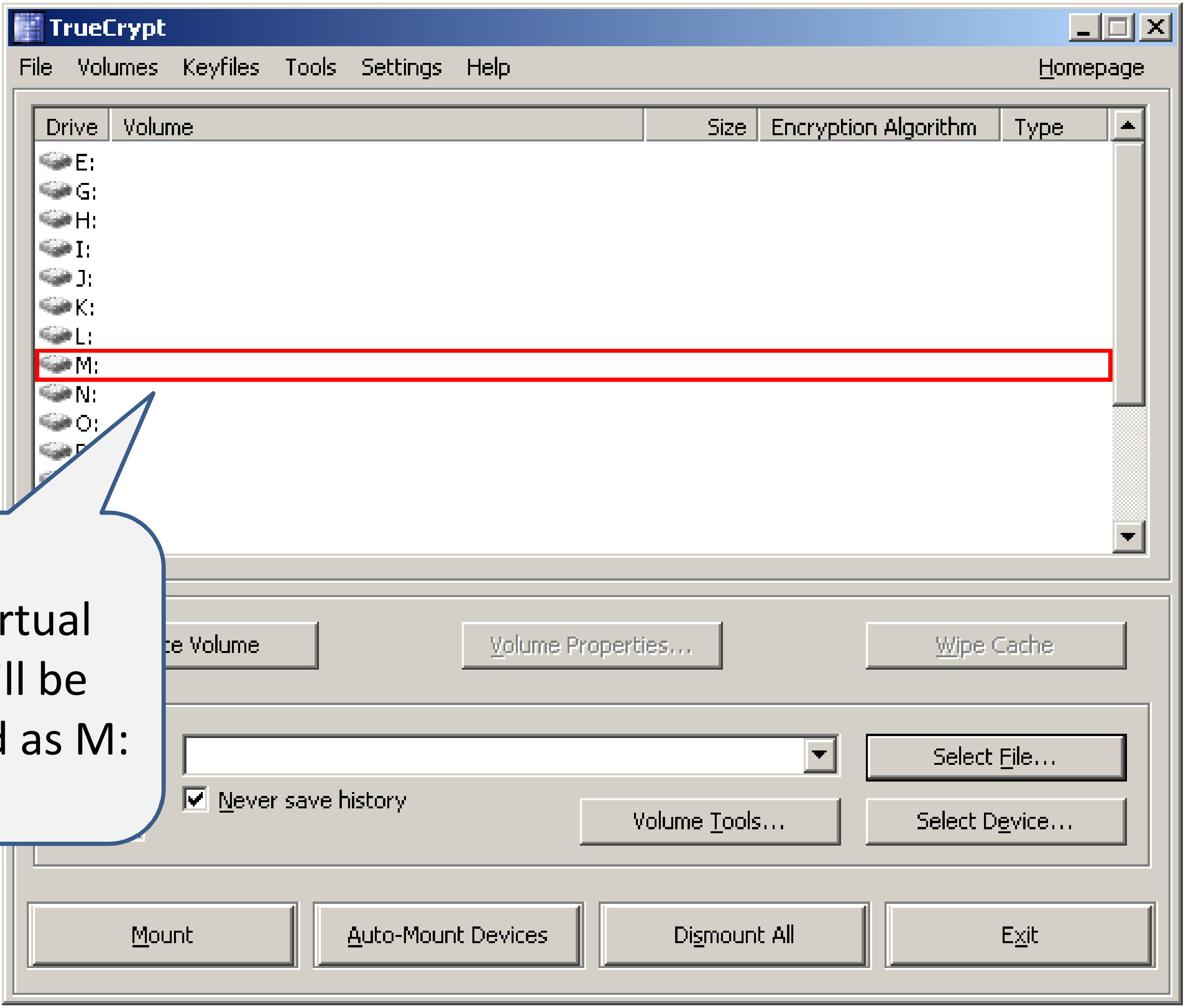
TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.



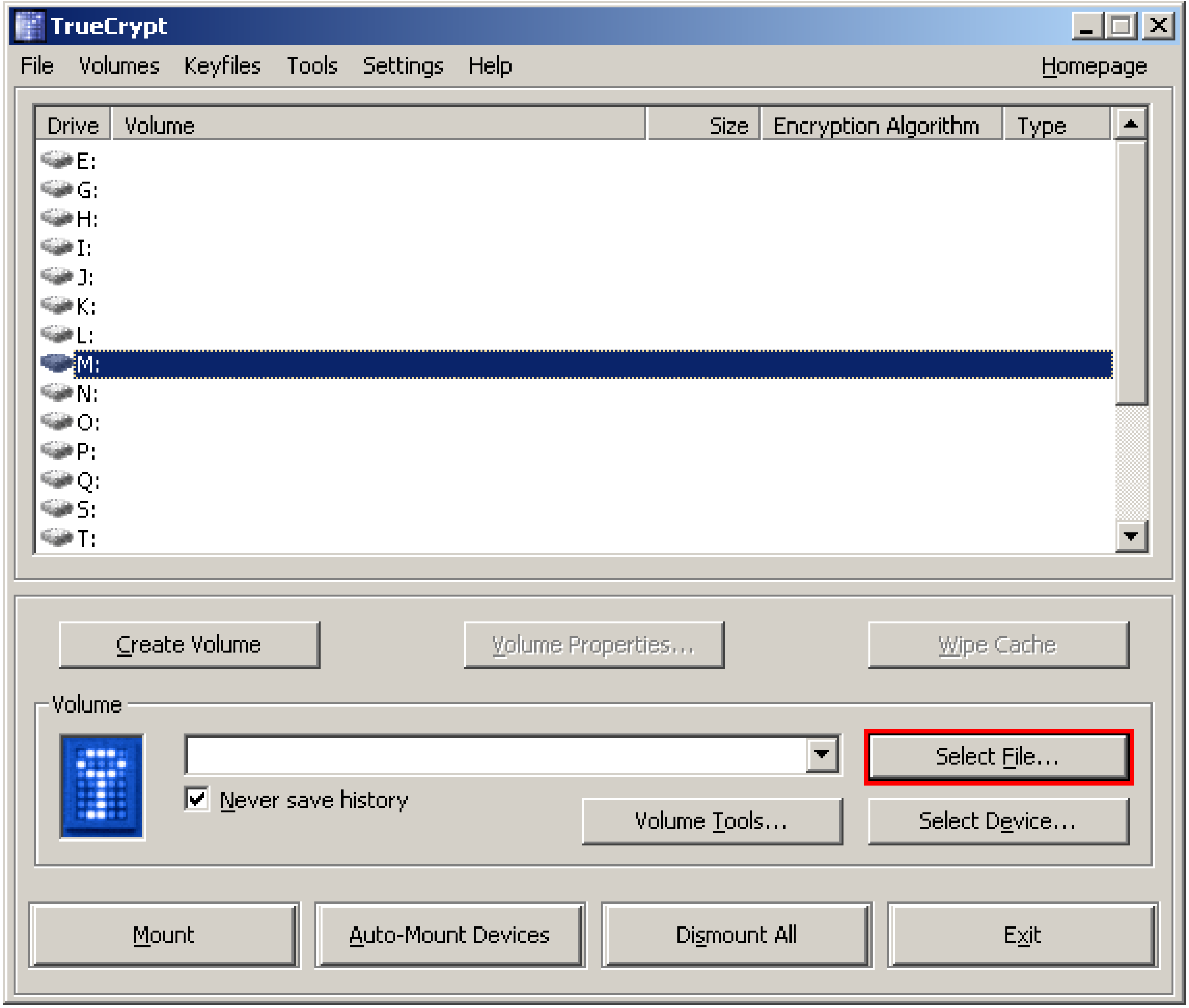
Volume Created

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

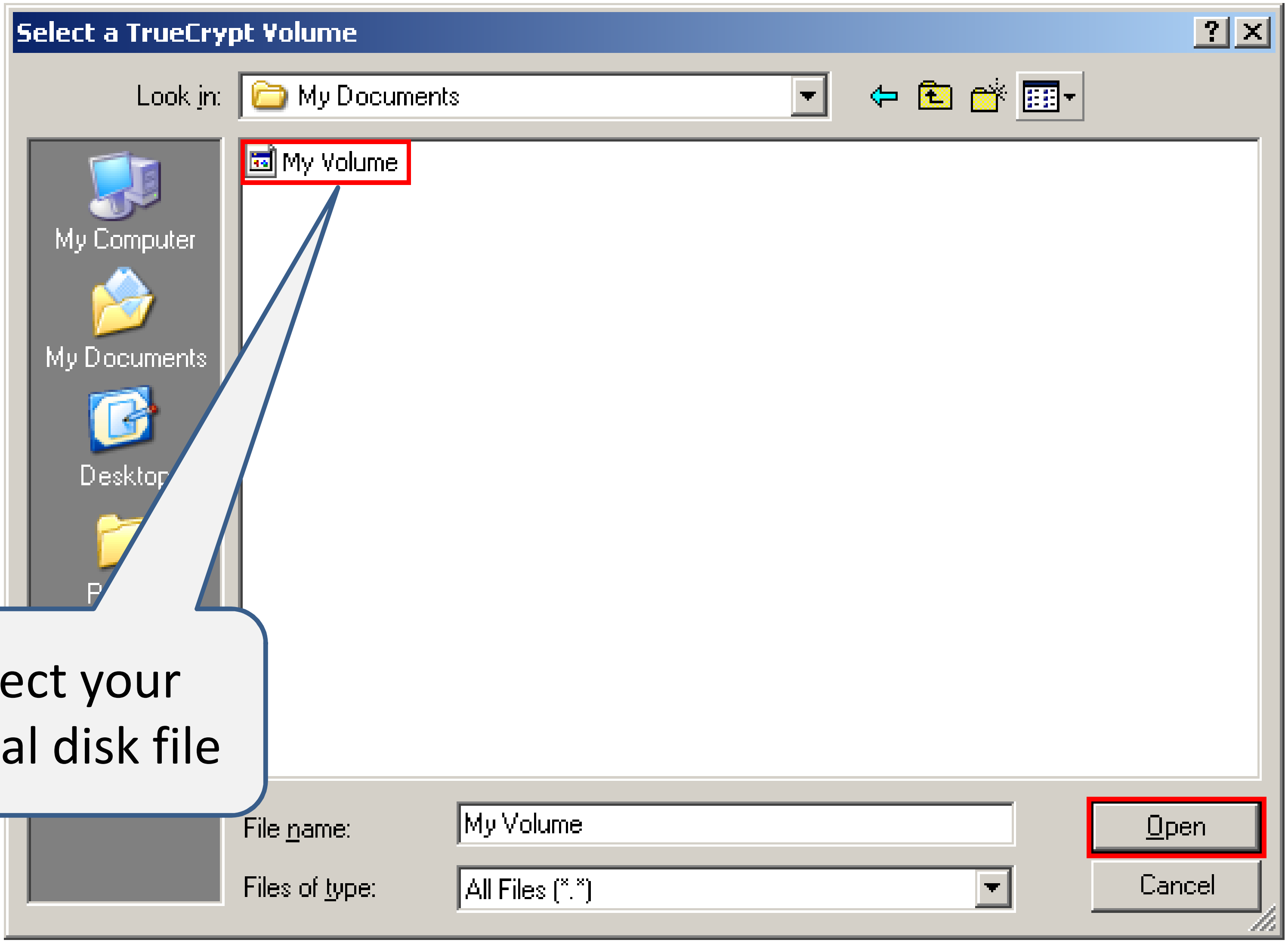


☑ Never save history

Your virtual disk will be mounted as M:



☑ Never save history

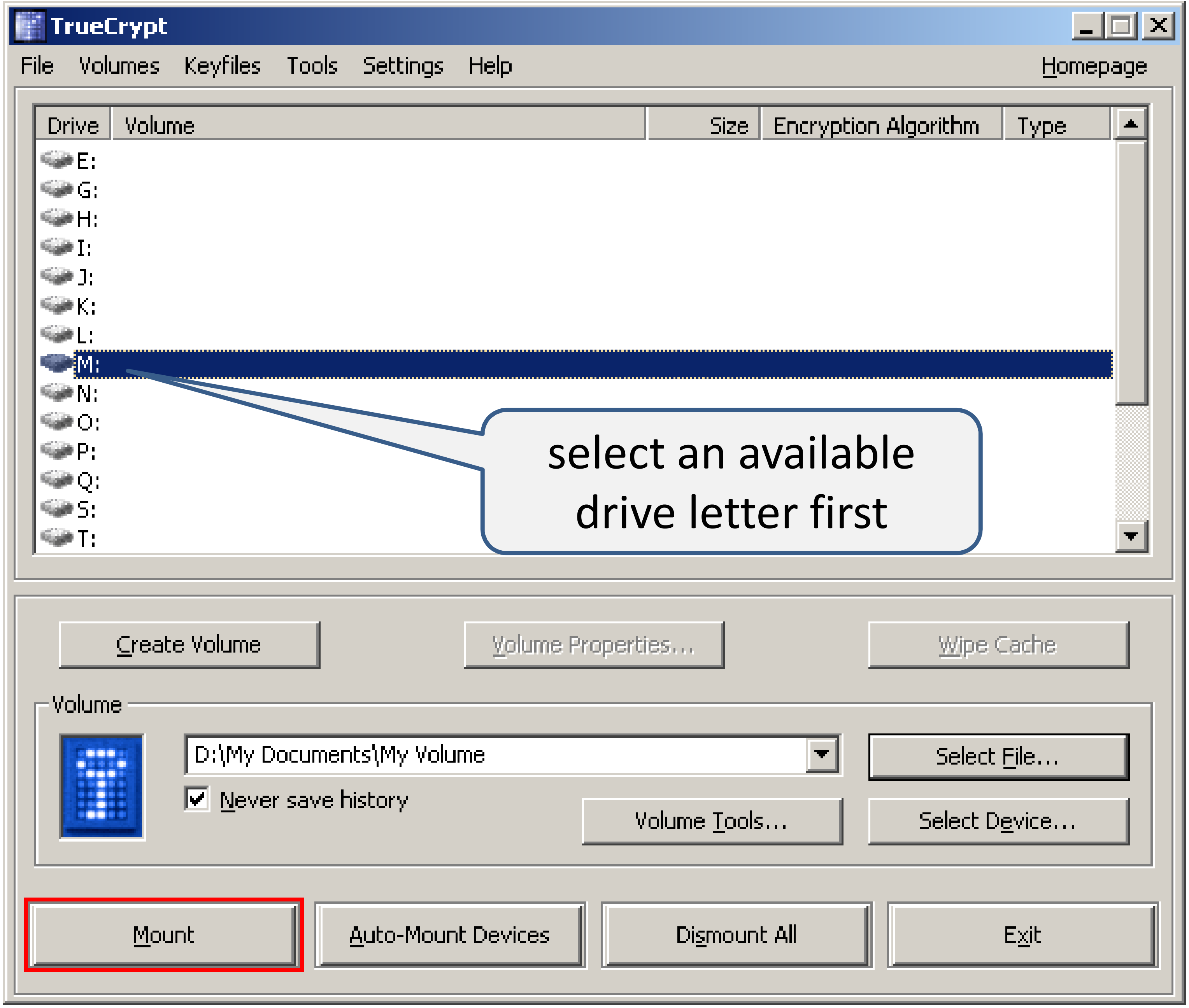


My Volume

File name: My Volume

Files of type: All Files (*.*)

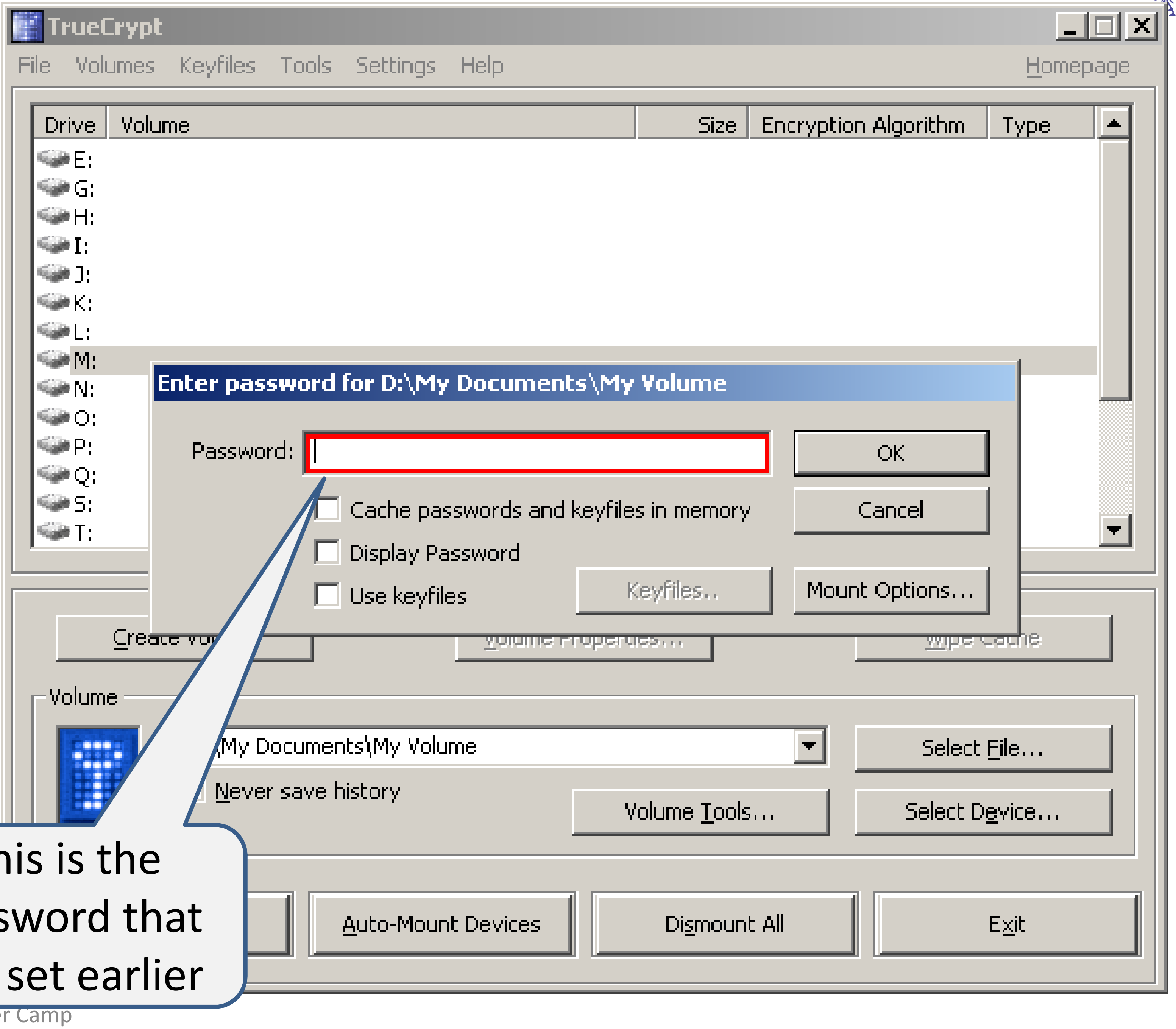
select your virtual disk file



D:\My Documents\My Volume

☑ Never save history

select an available drive letter first



Enter password for D:\My Documents\My Volume

Password:

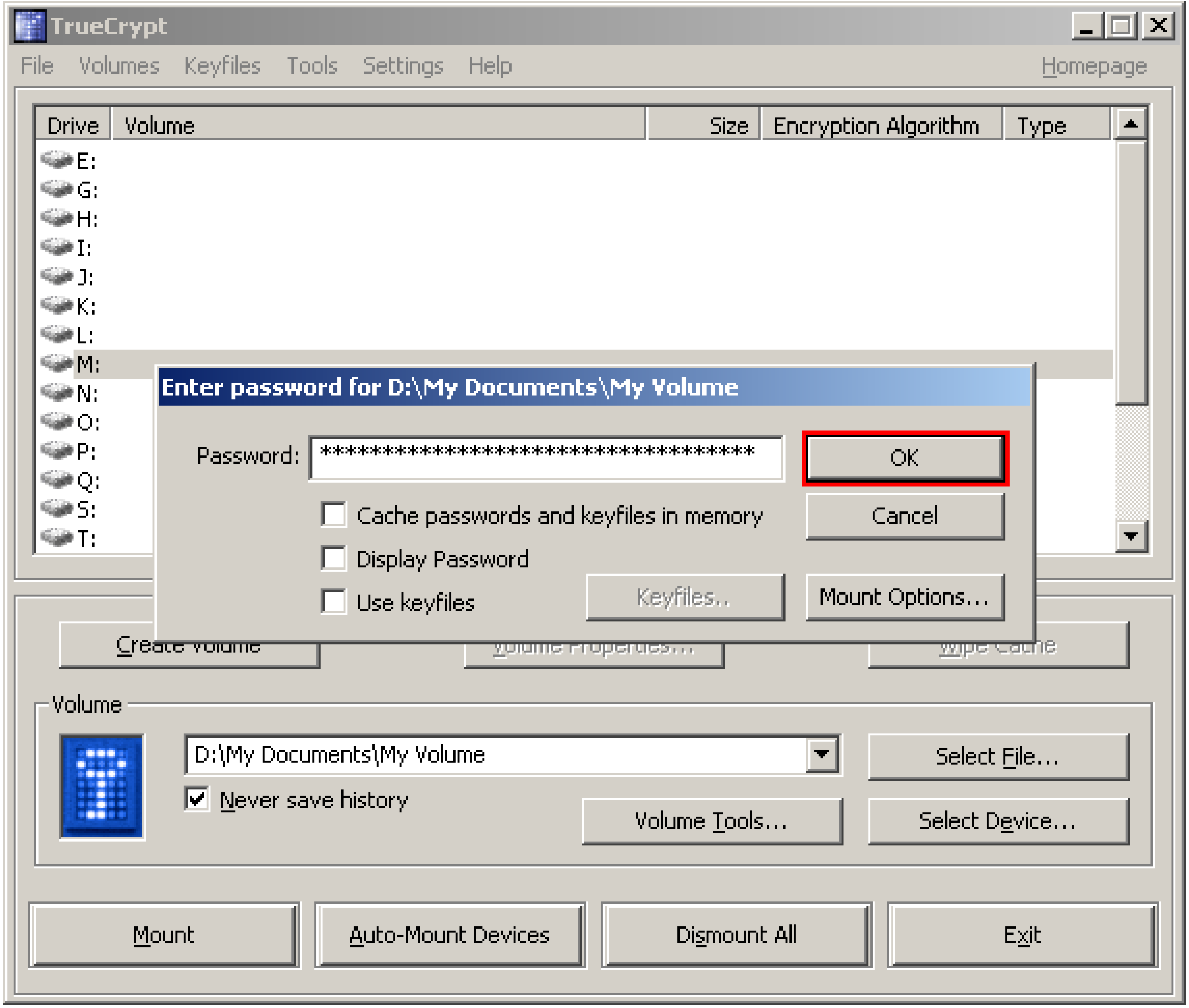
□ Cache passwords and keyfiles in memory

□ Display Password

□ Use keyfiles

Volume: \My Documents\My Volume

This is the password that you set earlier



Enter password for D:\My Documents\My Volume

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

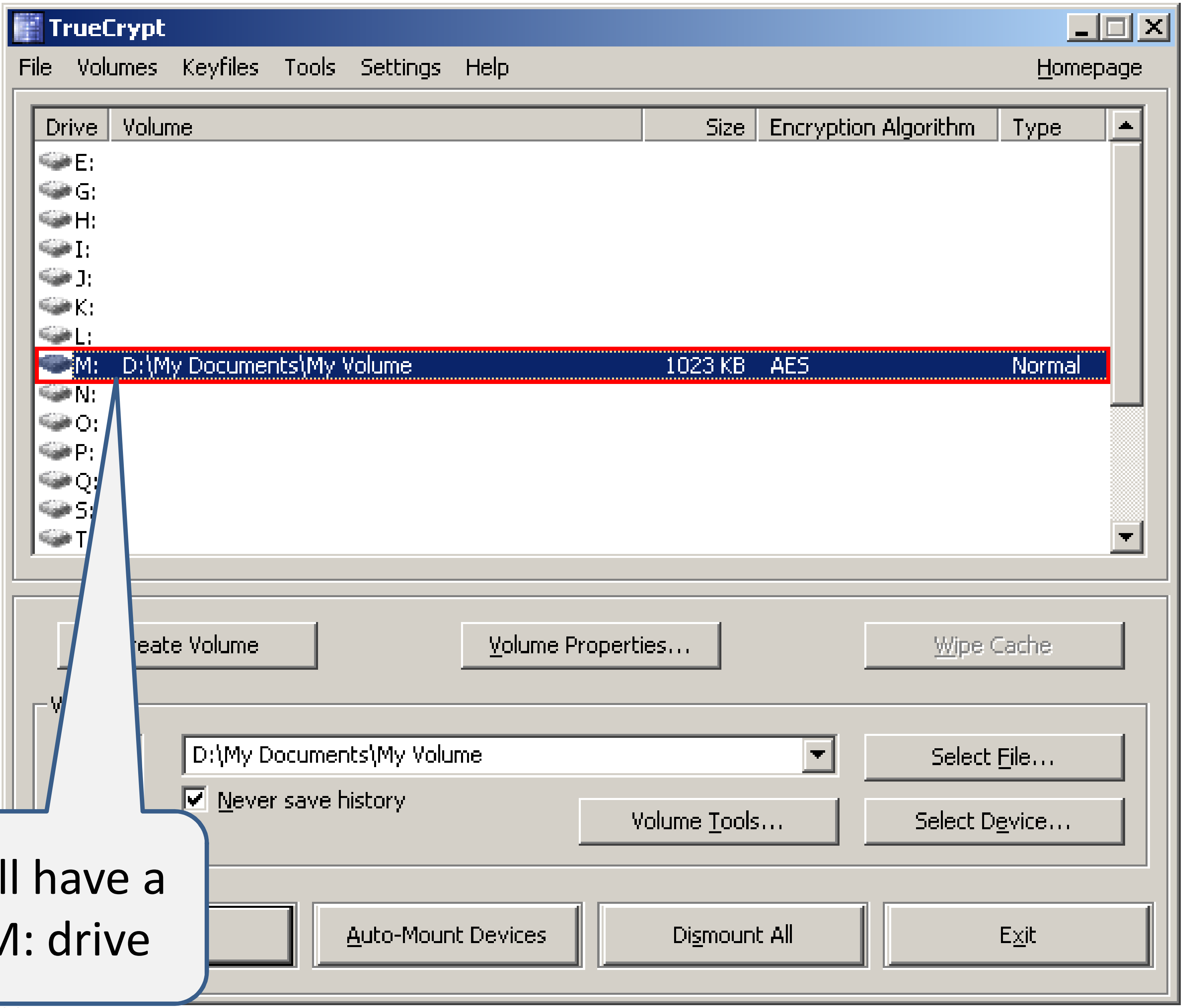
□ Cache passwords and keyfiles in memory

□ Display Password

□ Use keyfiles

Volume: D:\My Documents\My Volume

☑ Never save history

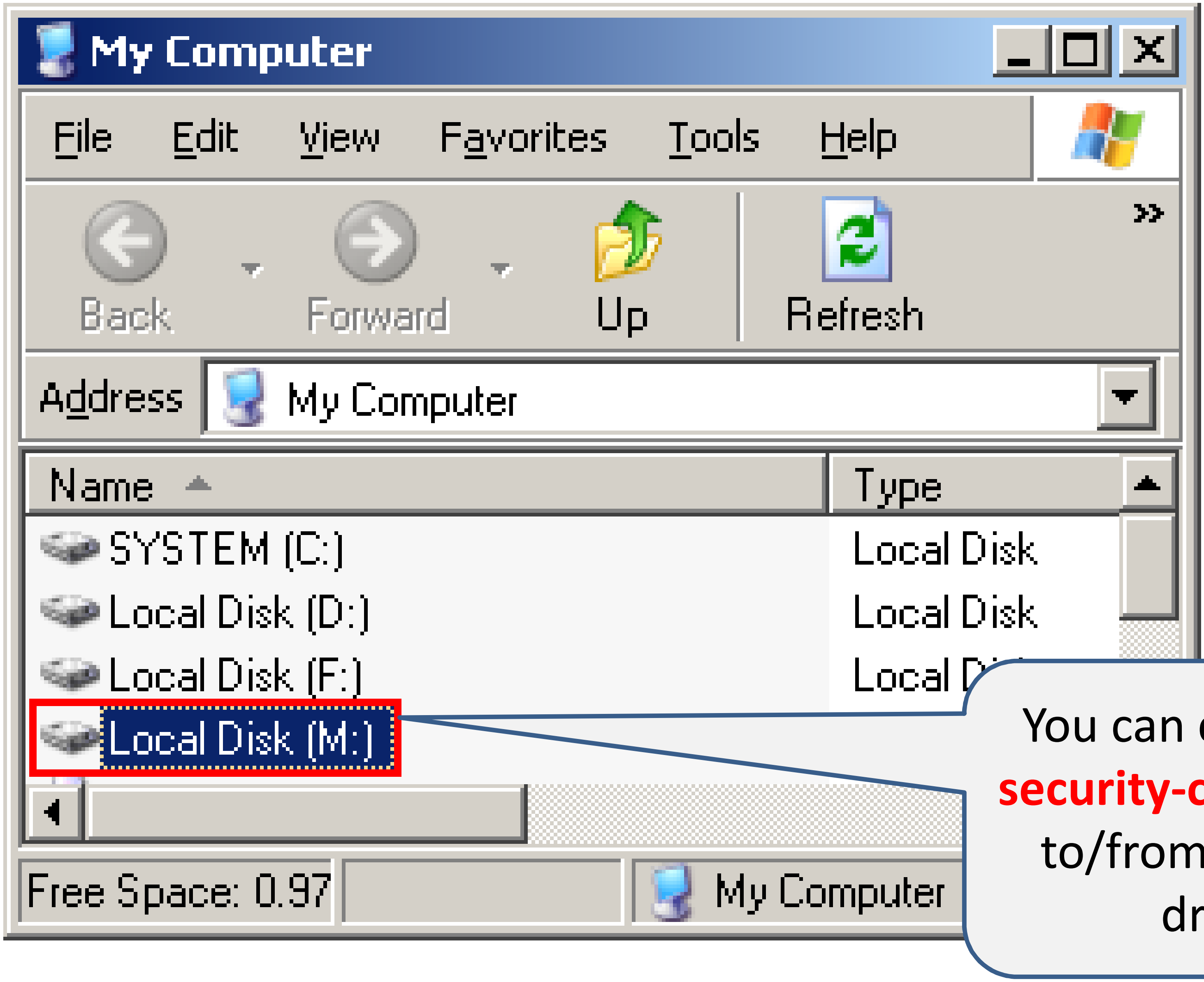


Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:	D:\My Documents\My Volume	1023 KB	AES	Normal
N:				
O:				
P:				
Q:				
S:				
T:				

D:\My Documents\My Volume

☑ Never save history

You will have a new M: drive

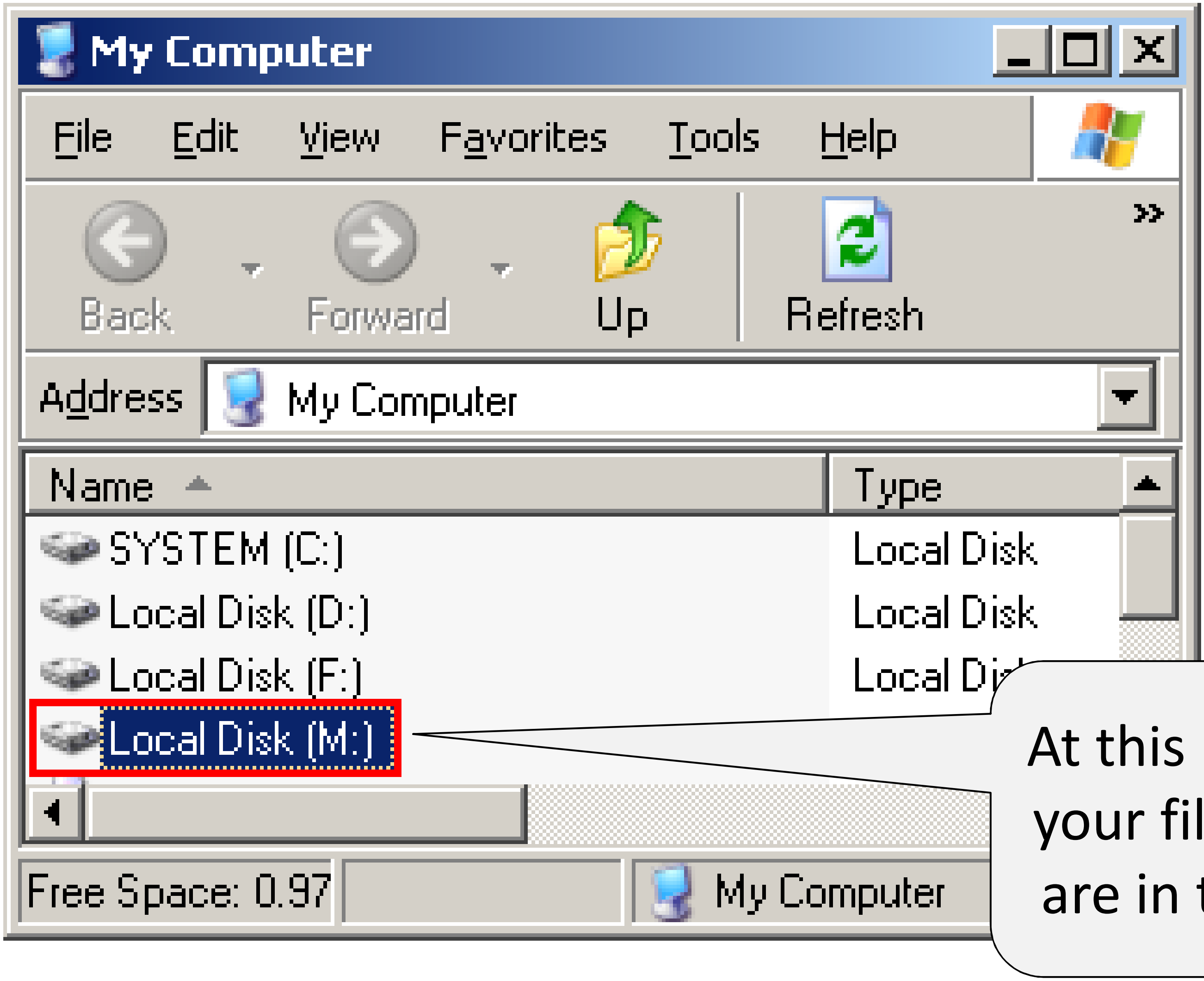


You can copy your **security-critical** files to/from your M: drive

Security-critical Files?

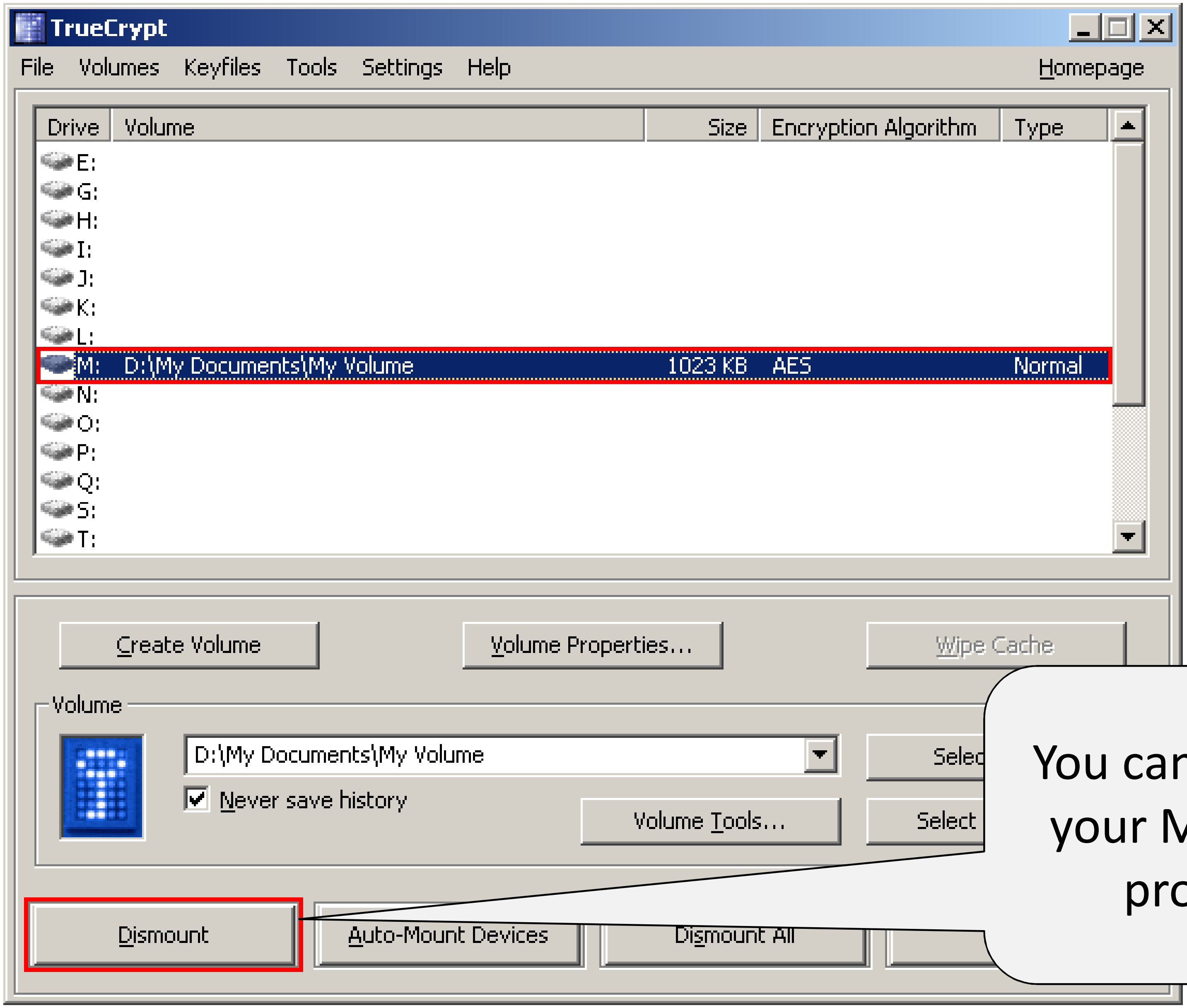
- Create a security-critical text file, finance.txt
  - Save the following information to it
    - your SSN and credit numbers in it
    - Your online banking account information
    - Your utility bill accounts information
    - Your other “important” digital stuffs

- Save it to **M:** drive



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:				

Volume: D:\My Documents\My Volume

☑ Never save history

You can dismount your M: drive to protect it

Exercise

① Create a TrueCrypt virtual disk (filename: *your_first_name-last_name*)

② Create a text file, finance.txt, and save it to your virtual disk

③ Dismount your virtual disk

④ Examine file *your_first_name-last_name* to see whether you can find any information about finance.txt

⑤ Copy *your_first_name-last_name* to c:\tmp

⑥ Mount c:\tmp\ *your_first_name-last_name* (the new copy)

⑦ 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?

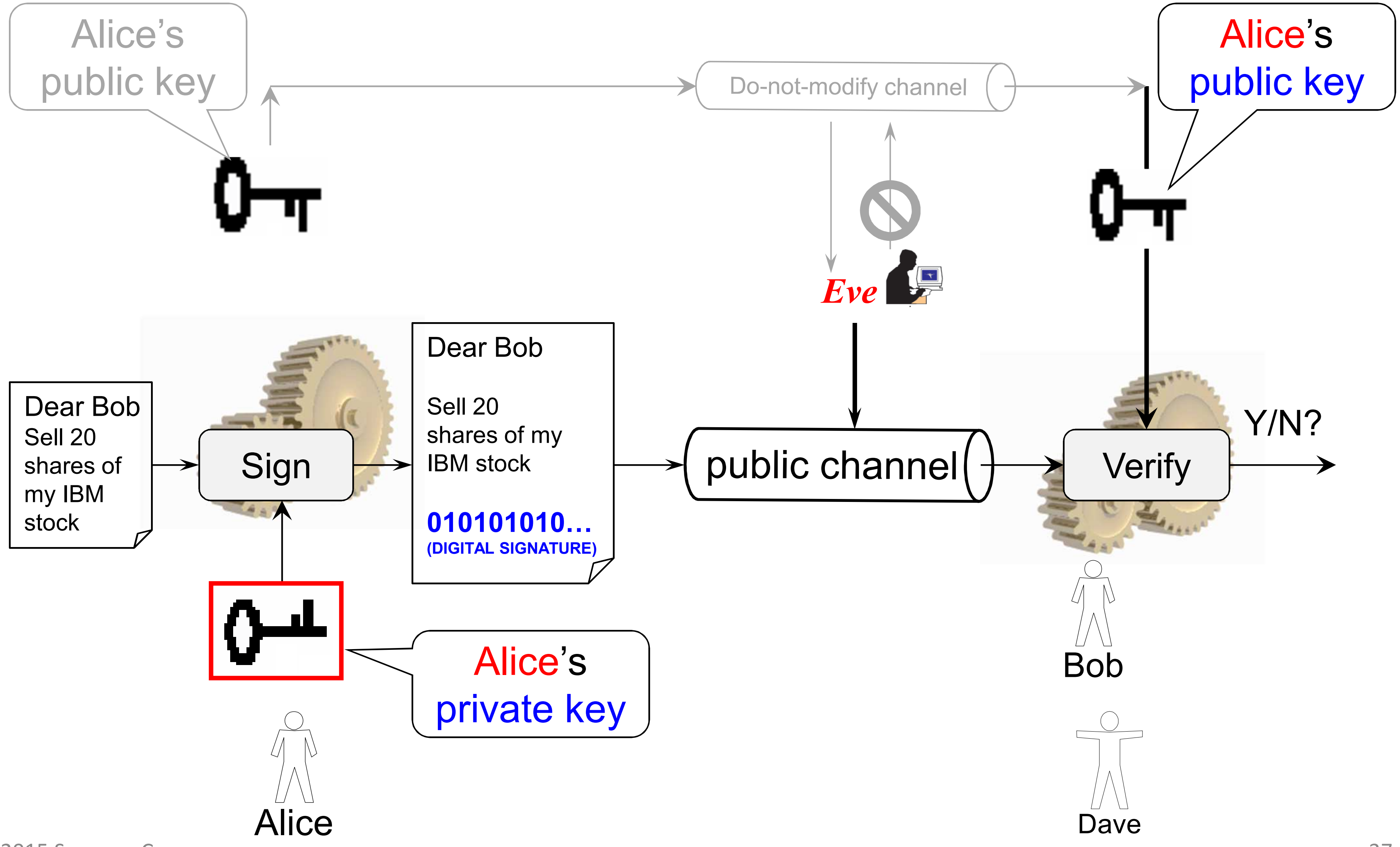
Warning

- 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!

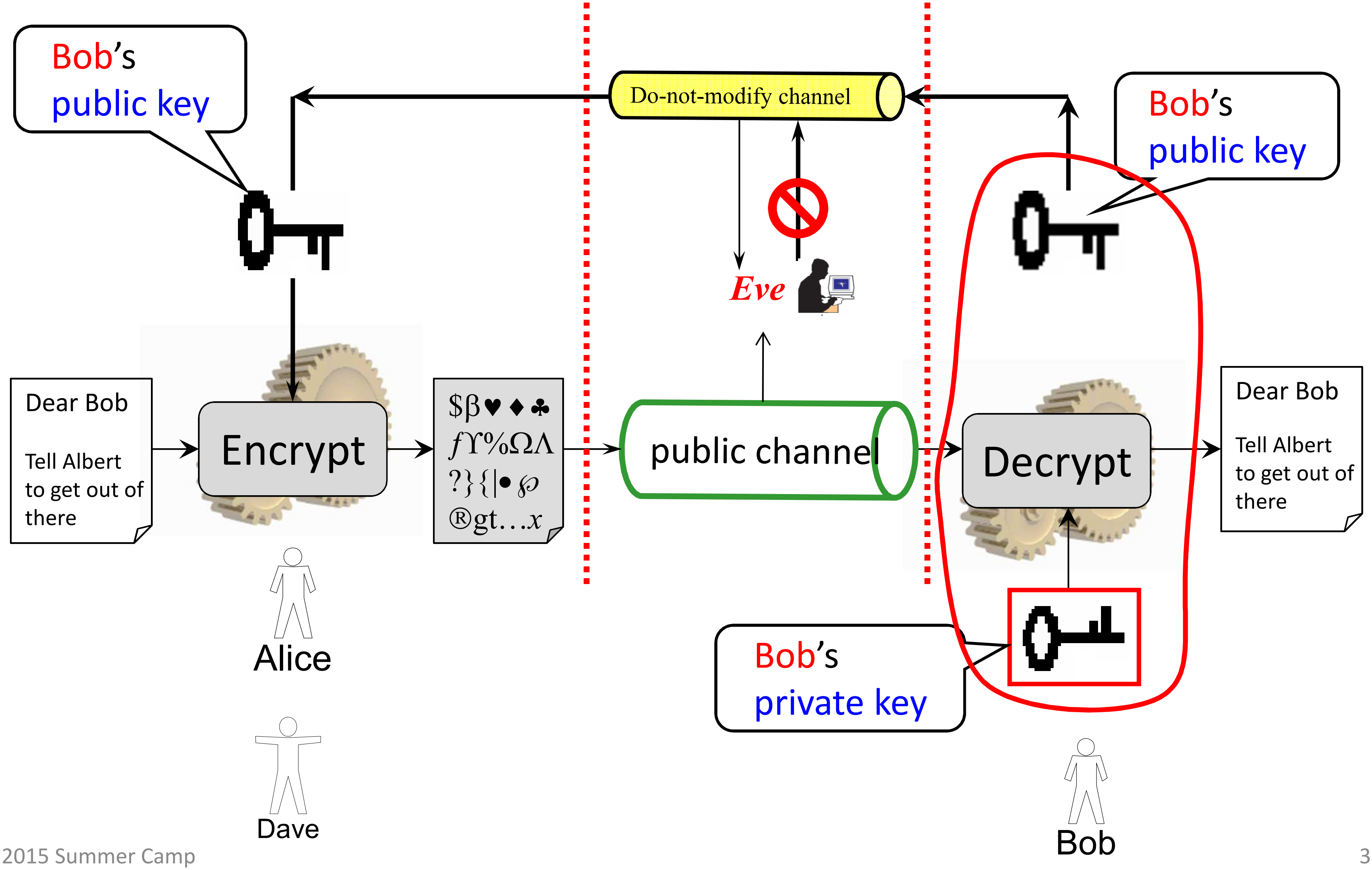
Road Map

- Practice
  - ❶Truecrypt
  - ❷GPG
  - ❸BitLocker

Public Key Digital Signature



Public Key Encryption



Bob's public key

Do-not-modify channel

Bob's public key

Eve

Dear Bob

Tell Albert to get out of there

Encrypt

$β♥♦♣ ƒϒ%ΩΛ ?}{|•℘ ®gt…x

public channel

Decrypt

Dear Bob

Tell Albert to get out of there

Alice

Bob's private key

Dave

Bob

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

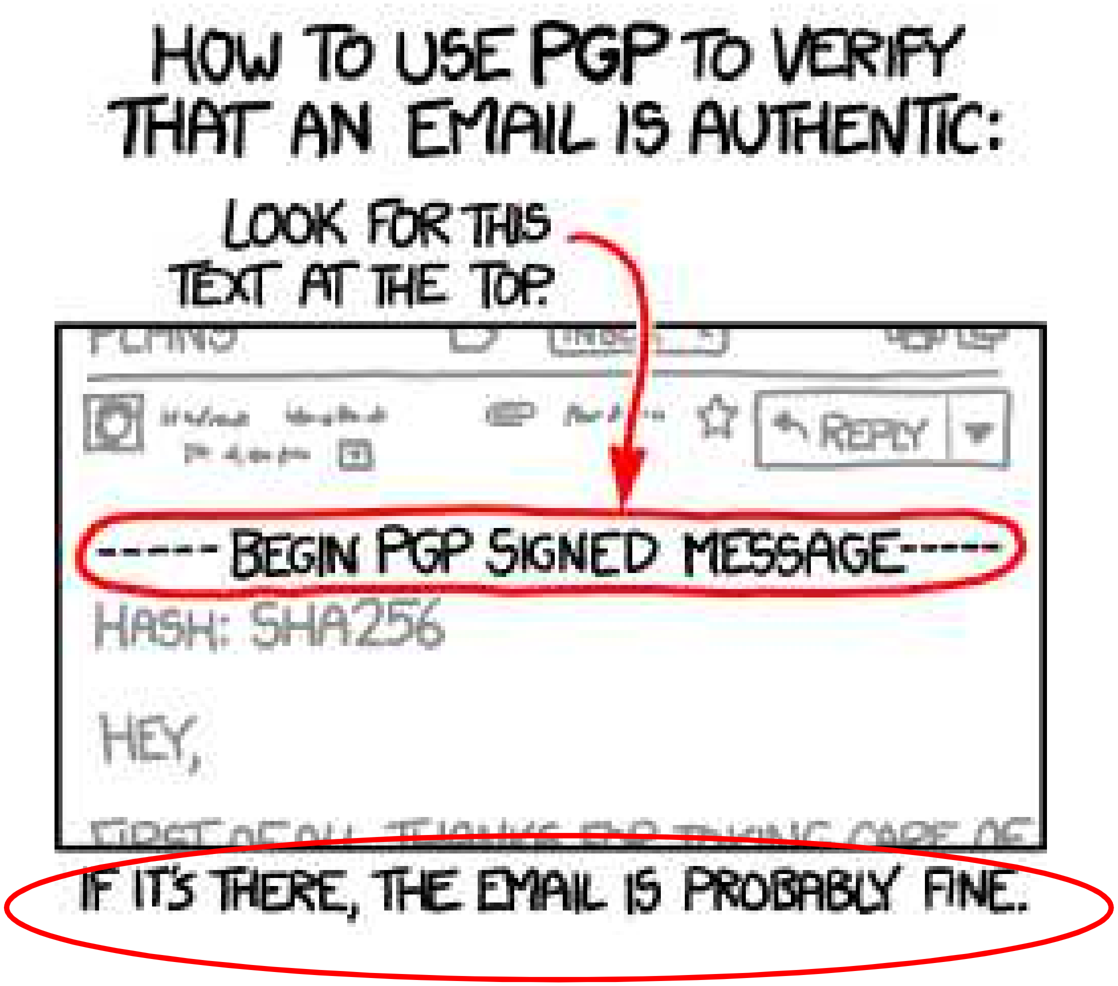
  Xunhua Wang, PhD
  Department of Computer Science
  James Madison University
  E-mail: wangxx@jmu.edu
  Tel: 540-568-3668

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

- Digital signature

  01110011001…

Verify an Email?


HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP.
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

What if I Want to…

- Encryption/sign a single file/email?

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

Step 1

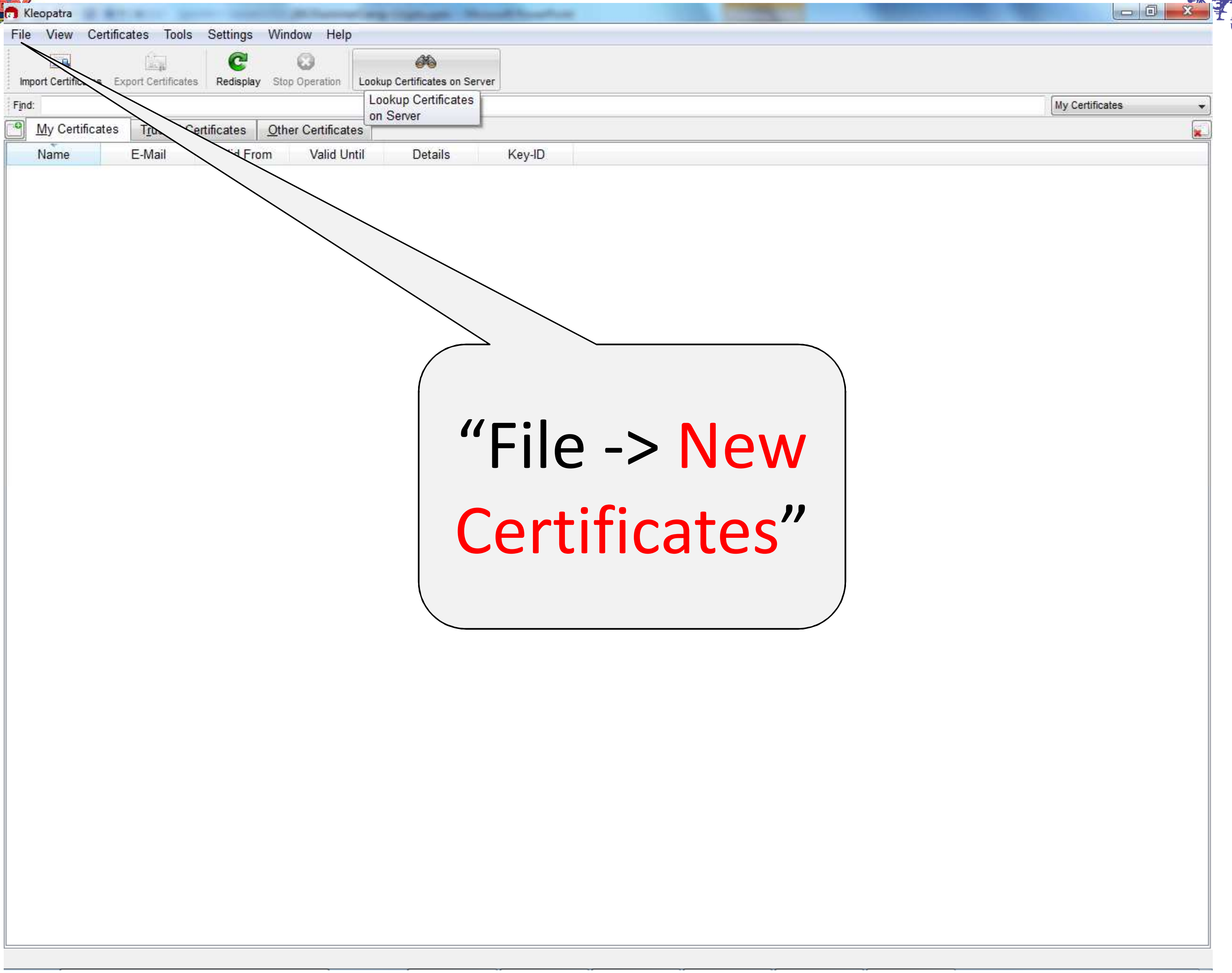
- Download Gpg4win and install it on your Windows 2003 VM
  - http://gpg4win.org/

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

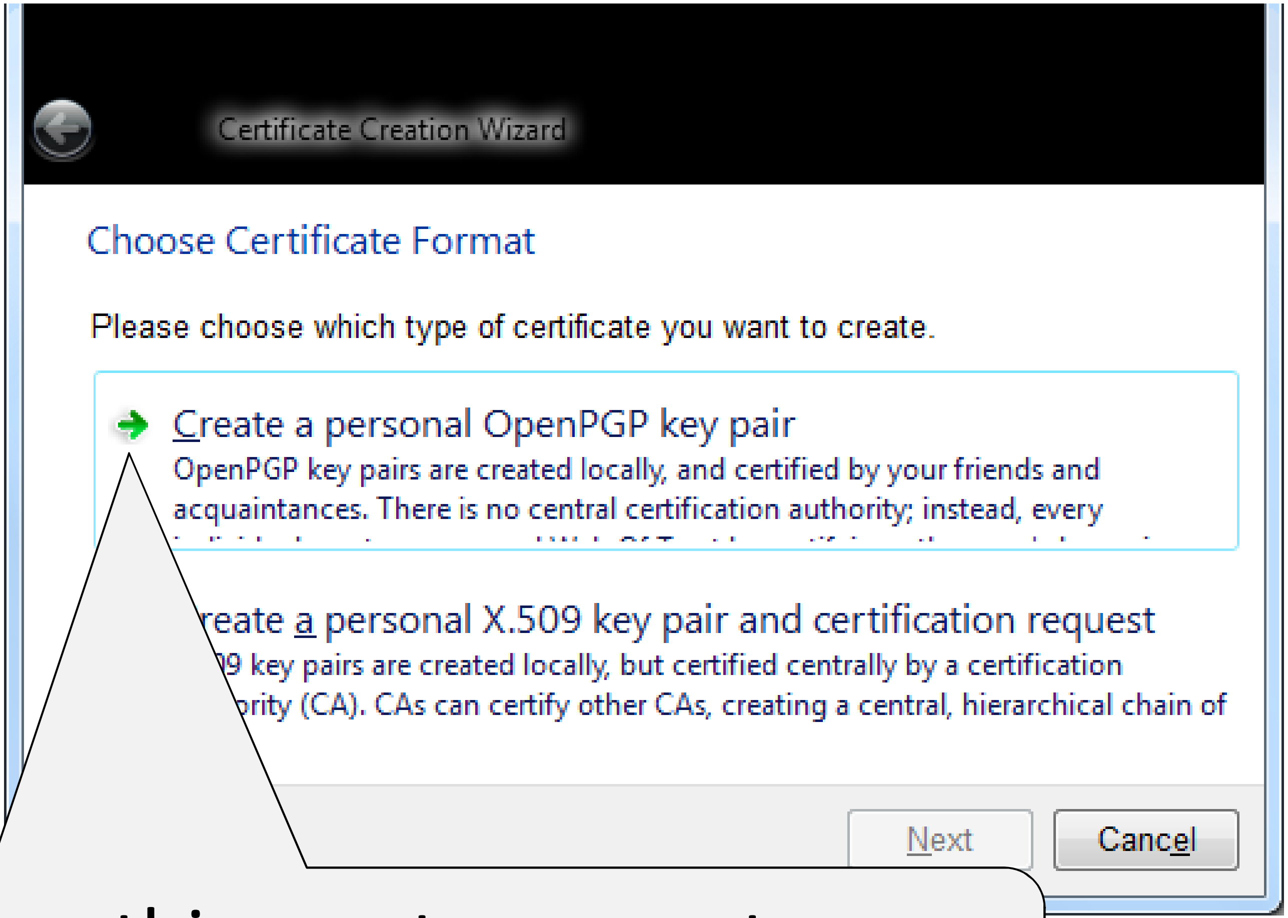
Step 2

- 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”



Choose Certificate Format

Please choose which type of certificate you want to create.

Create a personal OpenPGP key pair

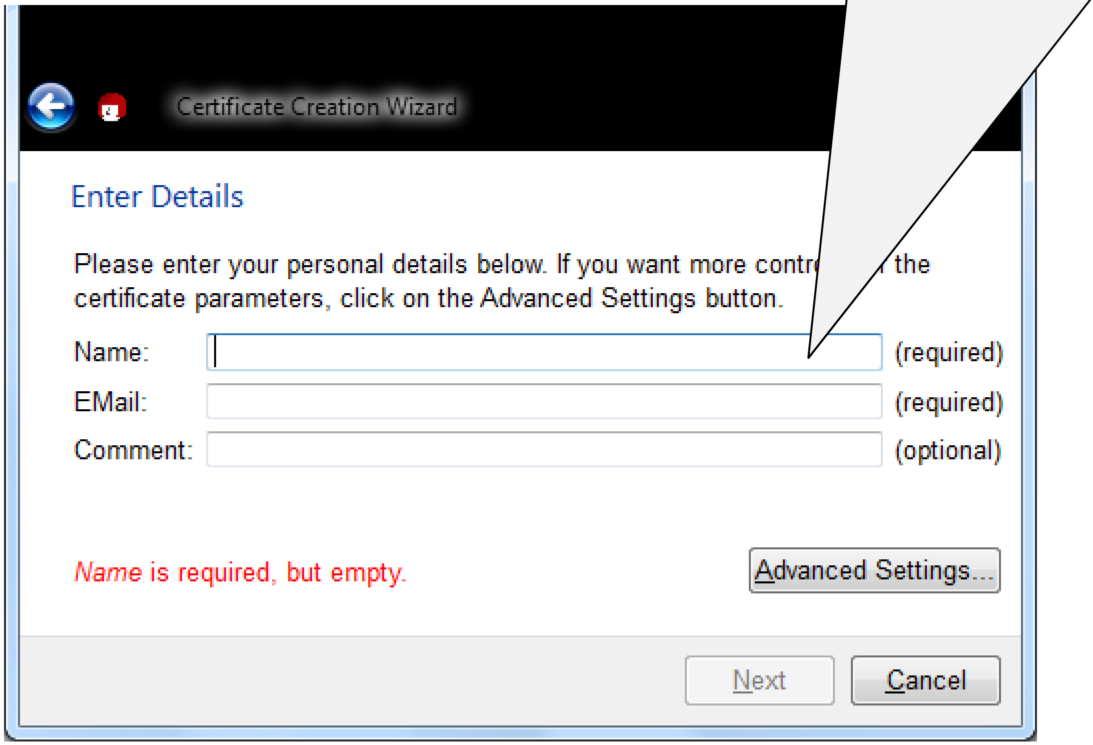
OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every

reate a personal X.509 key pair and certification request

09 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



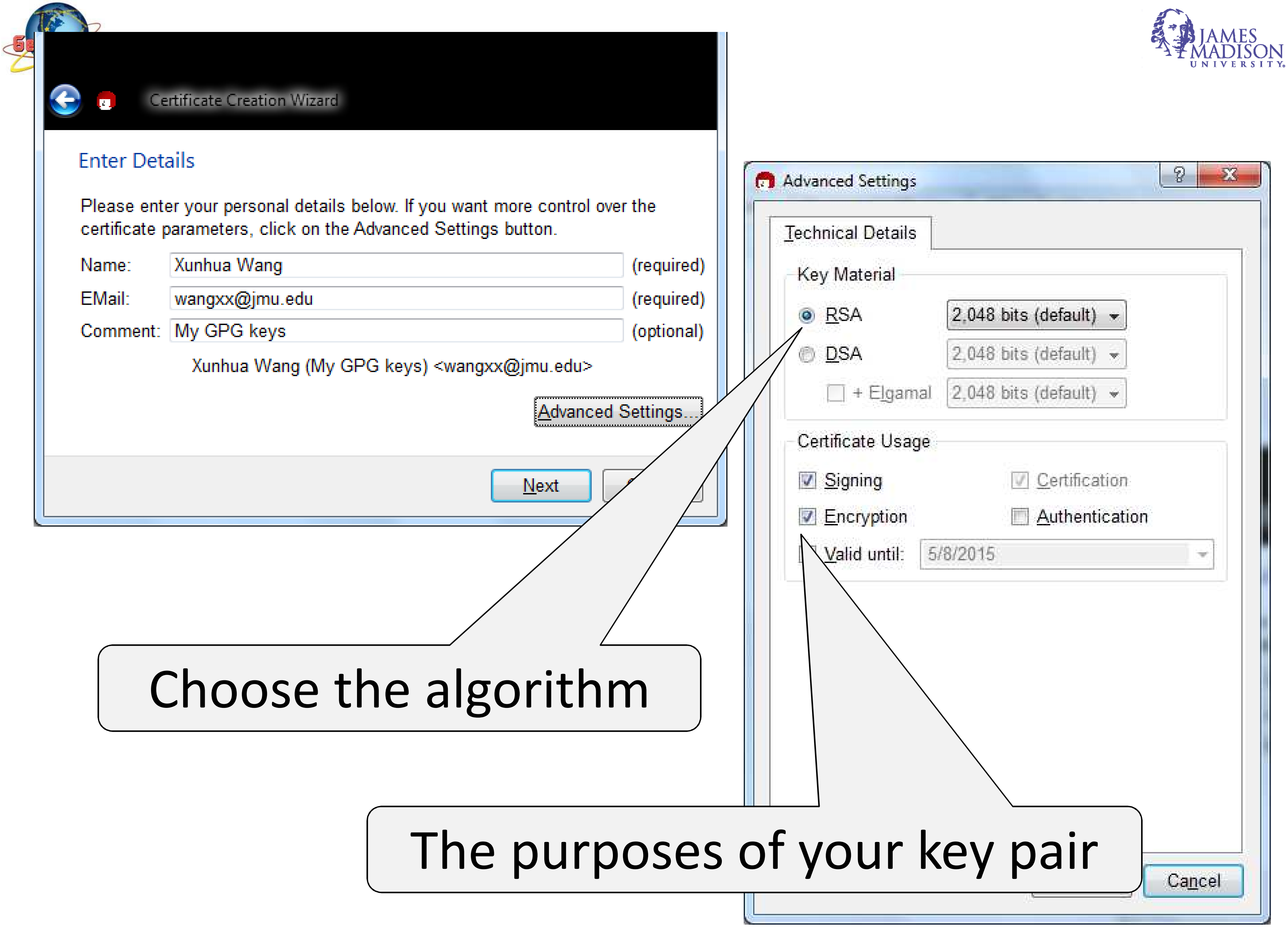
Certificate Creation Wizard

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

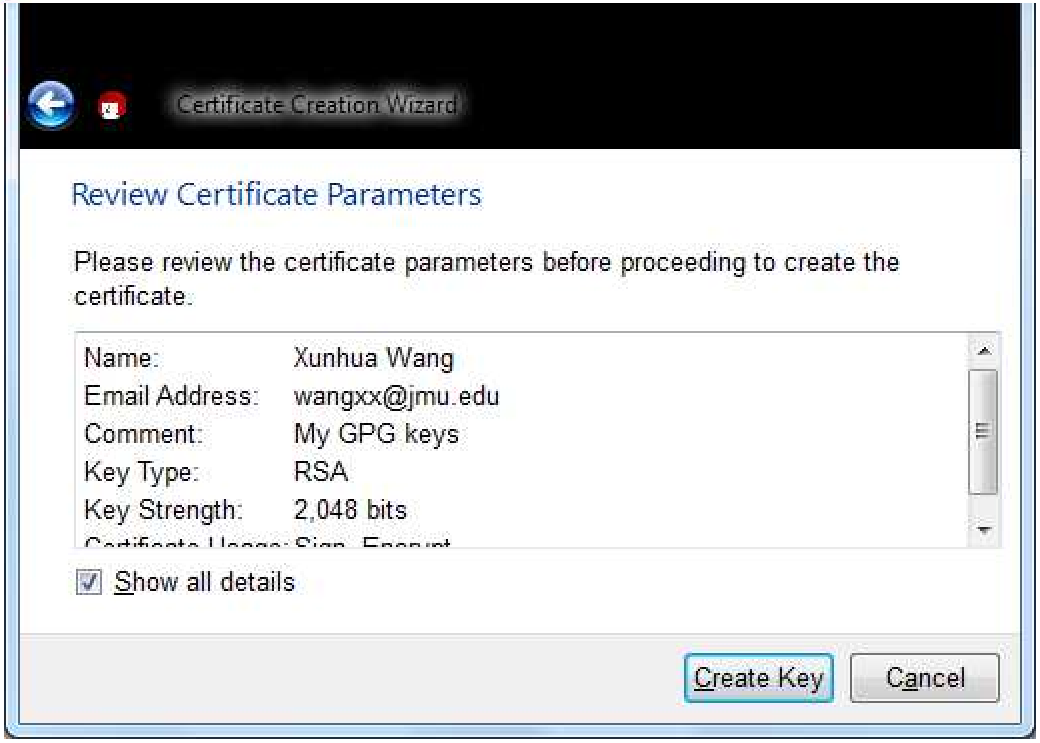
☑ Signing ☑ Certification

☑ Encryption □ Authentication

□ Valid until: 5/8/2015

Choose the algorithm

The purposes of your key pair

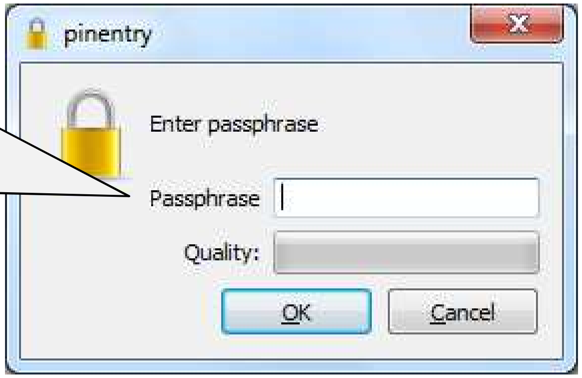


Review Certificate Parameters

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



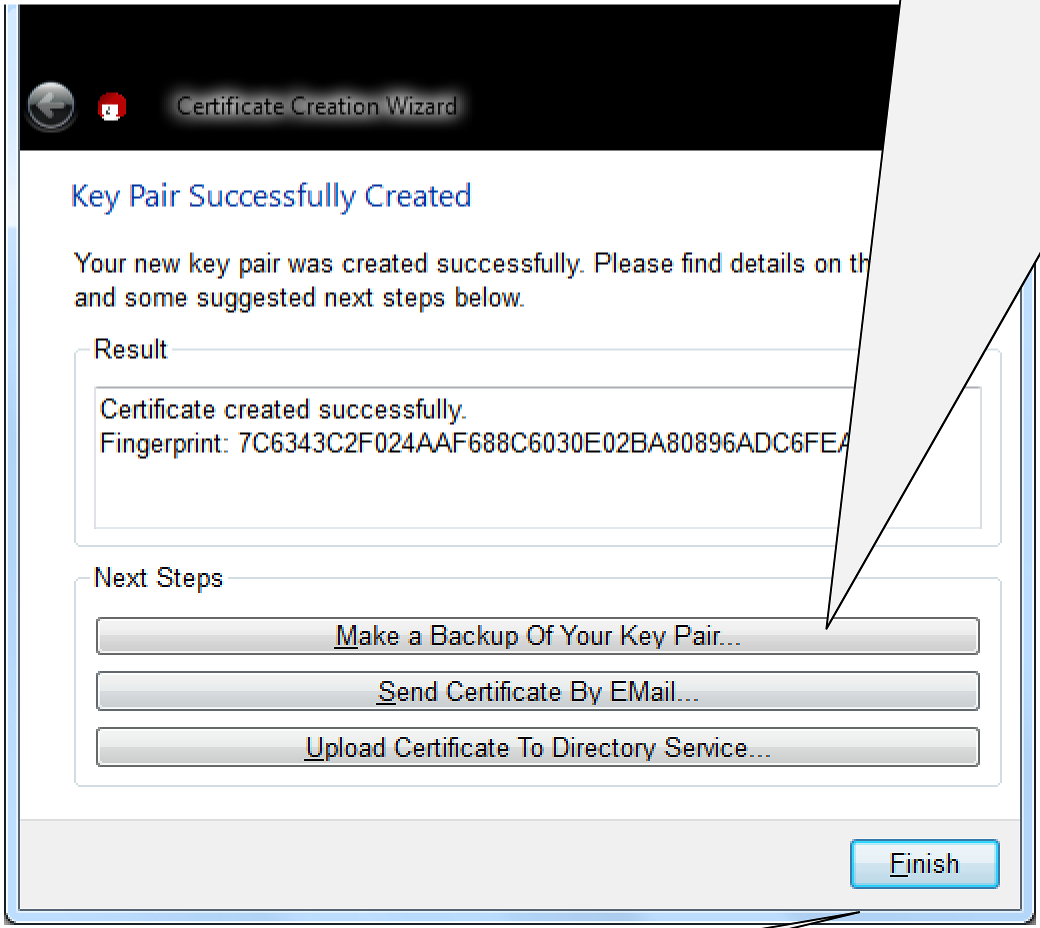
Enter passphrase

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

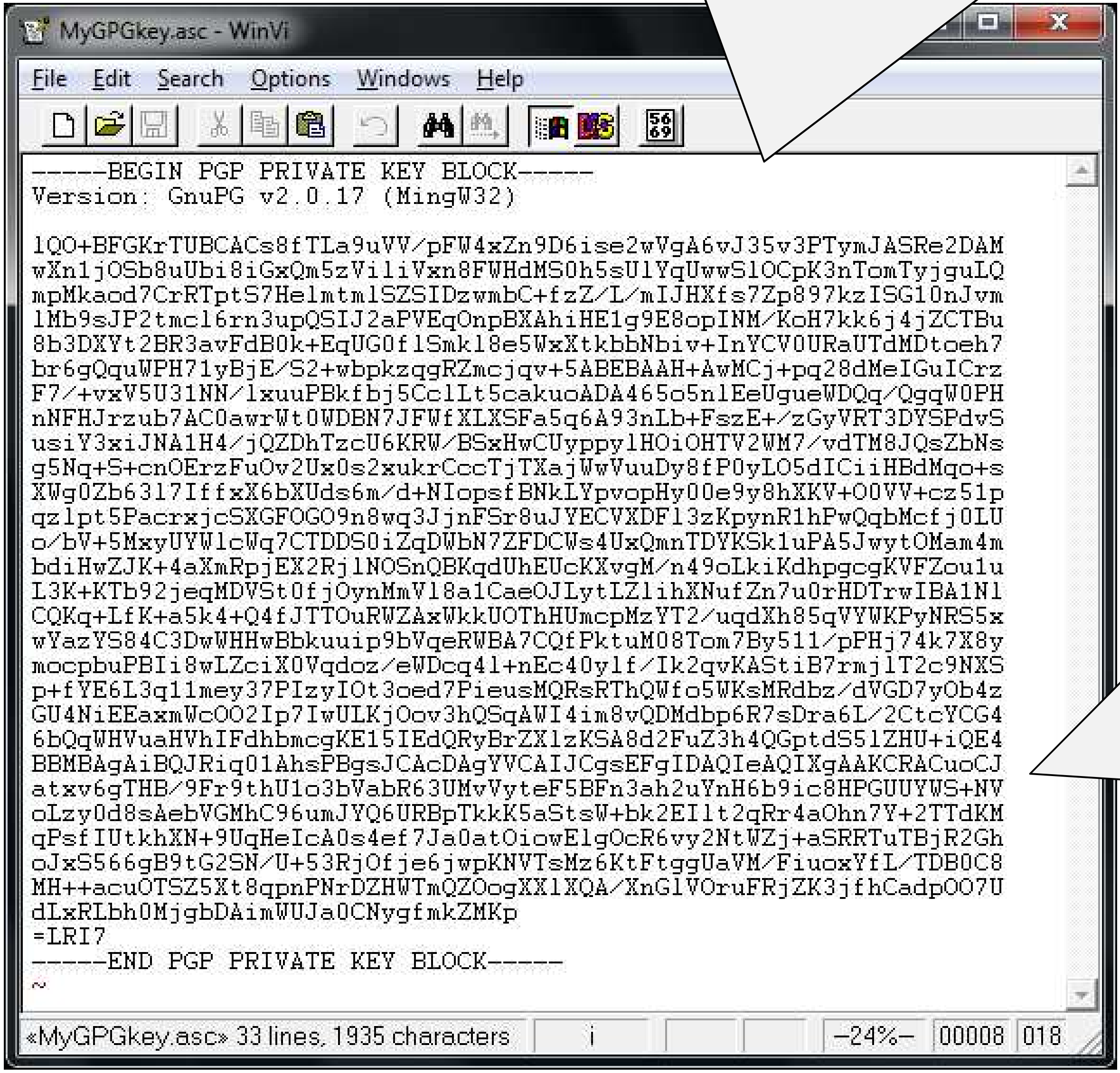
Certificate created successfully.
Fingerprint: 7C6343C2F024AAF688C6030E02BA80896ADC6FEA

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

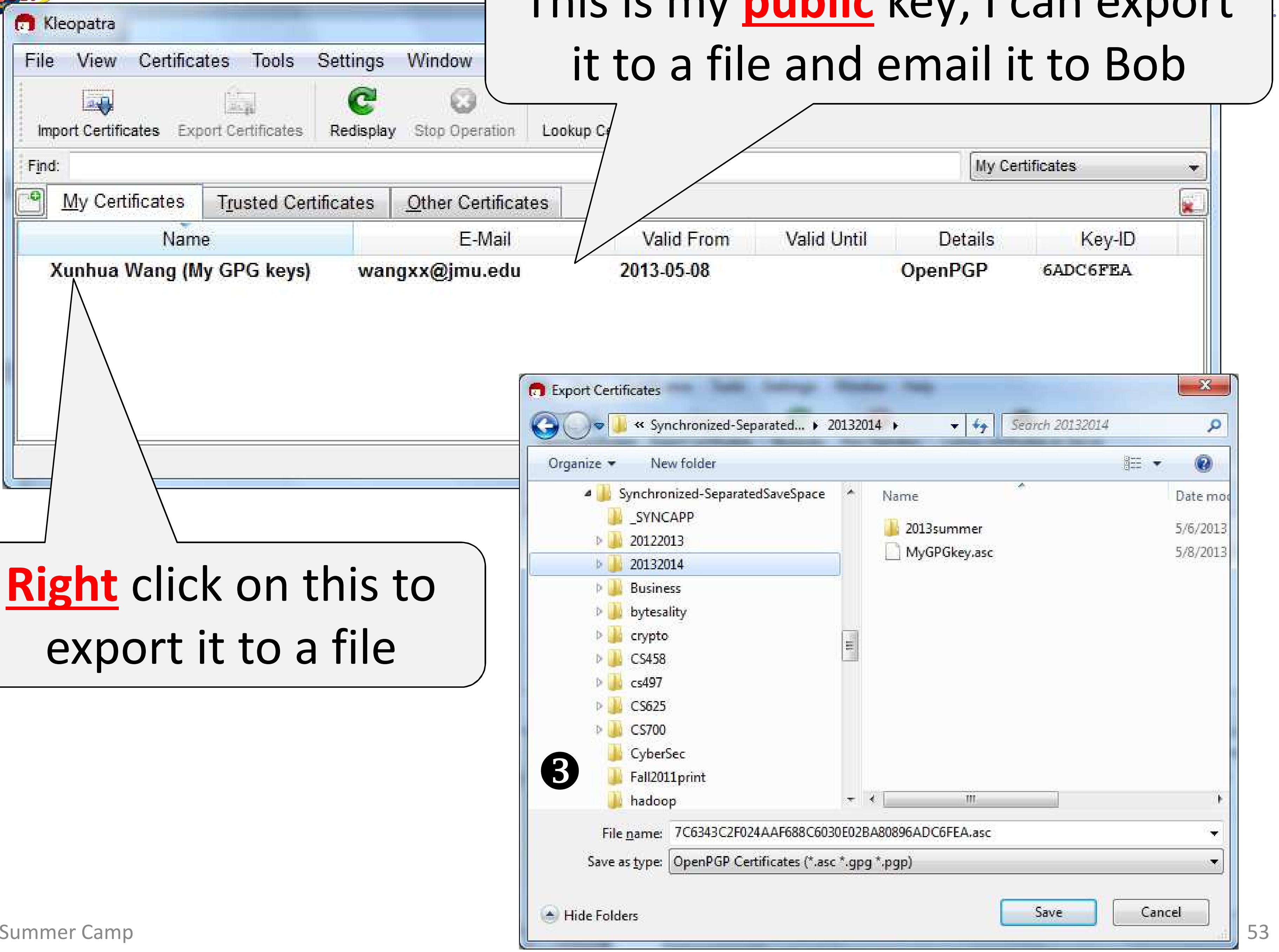

MyGPGkey.asc - WinVi
File Edit Search Options Windows Help
«MyGPGkey.asc» 33 lines, 1935 characters
i
–24%–
00008
018

```
-----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+fYE6L3q11mey37PIzyIOt3oed7PieusMQRsRThQWfo5WKsMRdbz/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-----
~
```

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

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



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

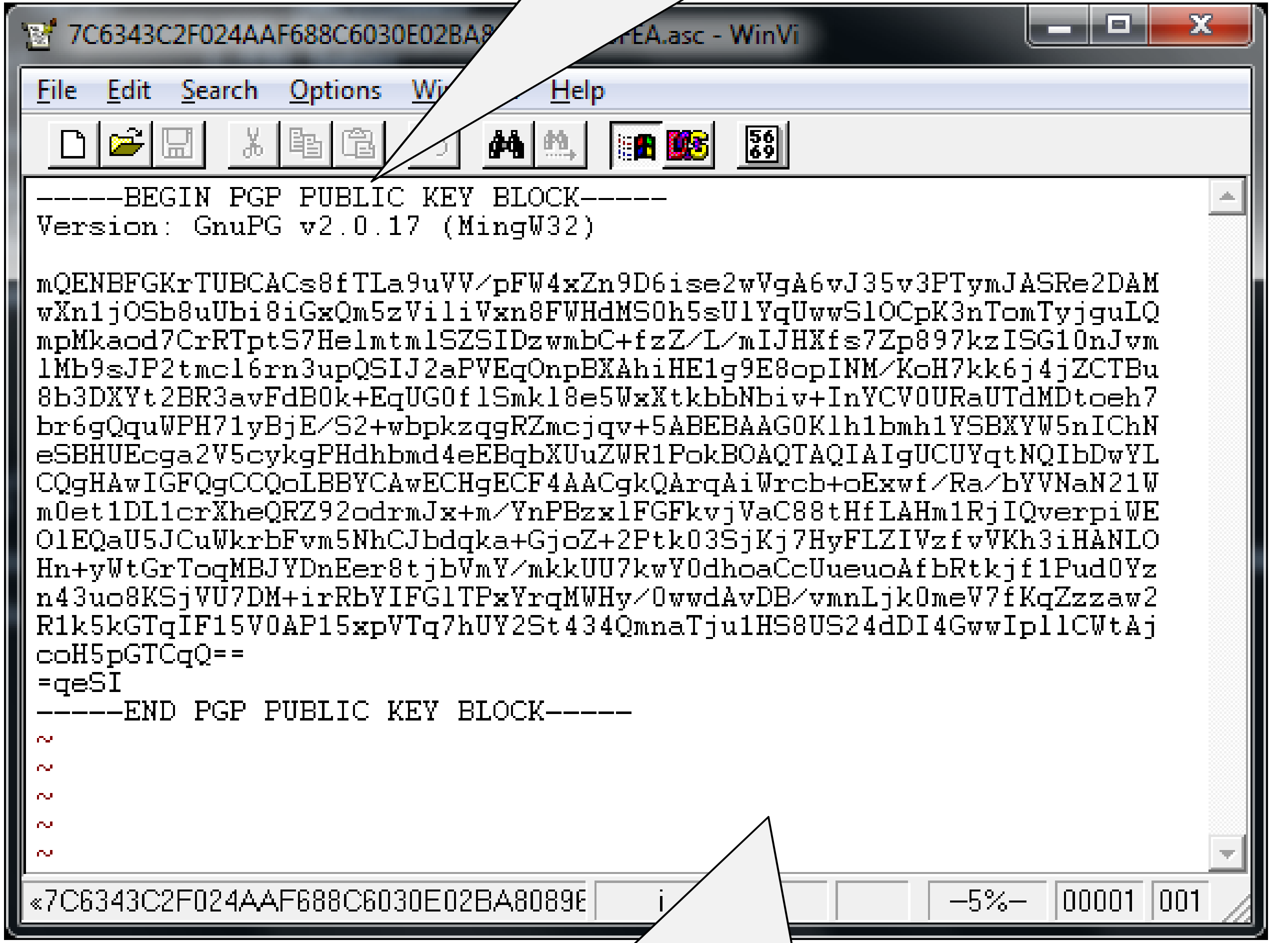
Name	Date mod
2013summer	5/6/2013
MyGPGkey.asc	5/8/2013

File name: 7C6343C2F024AAF688C6030E02BA80896ADC6FEA.asc

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

Right click on this to export it to a file

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


7C6343C2F024AAF688C6030E02BA8
EA.asc - WinVi
File
Edit
Search
Options
Wi
Help
«7C6343C2F024AAF688C6030E02BA8089E
i
-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-----
~
~
~
~
~
```

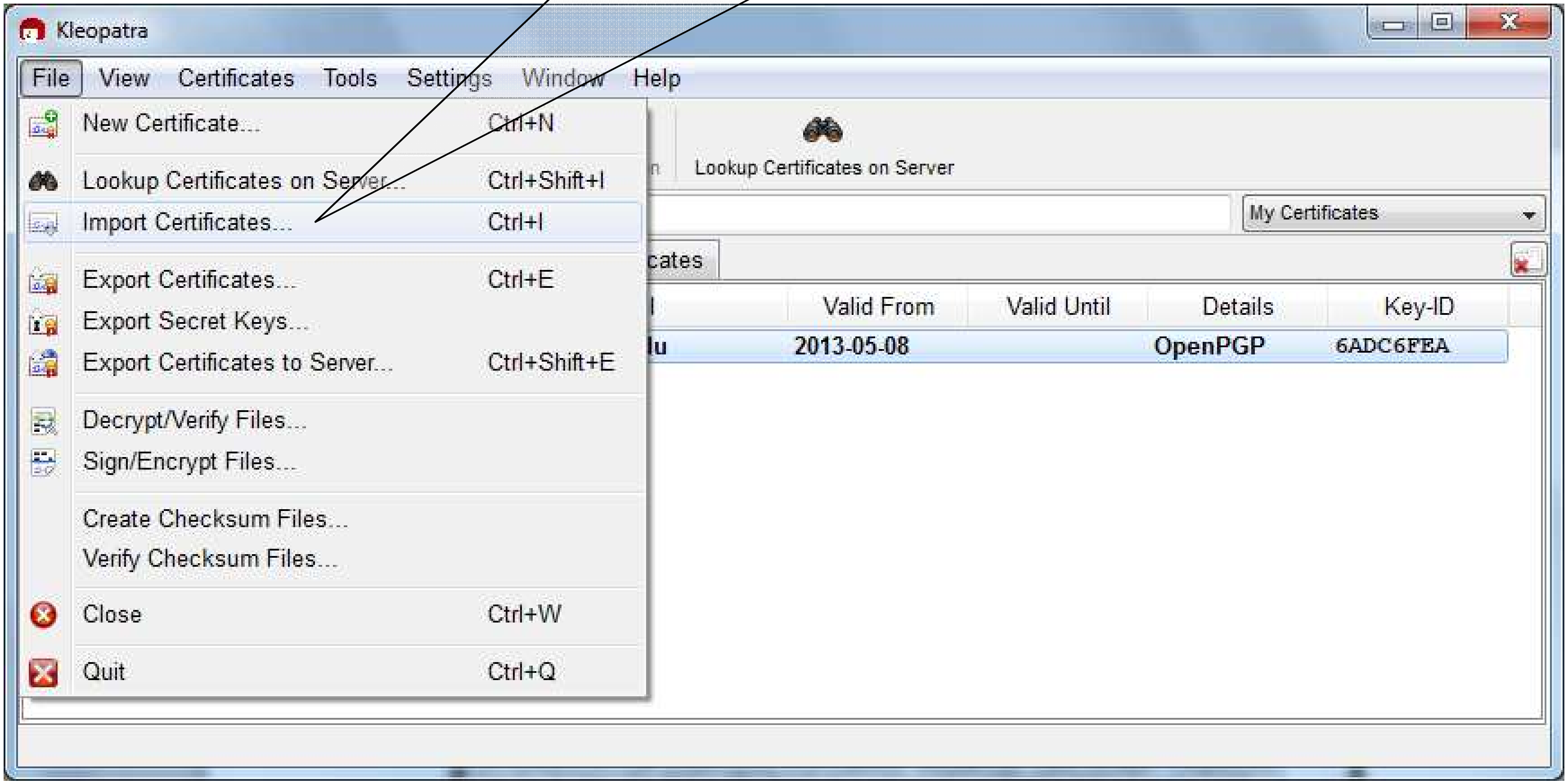
I can email it to my friends

Exercise #1 (1/2)

①Export your **<u>public</u>** key to a file and email it to the student next to you

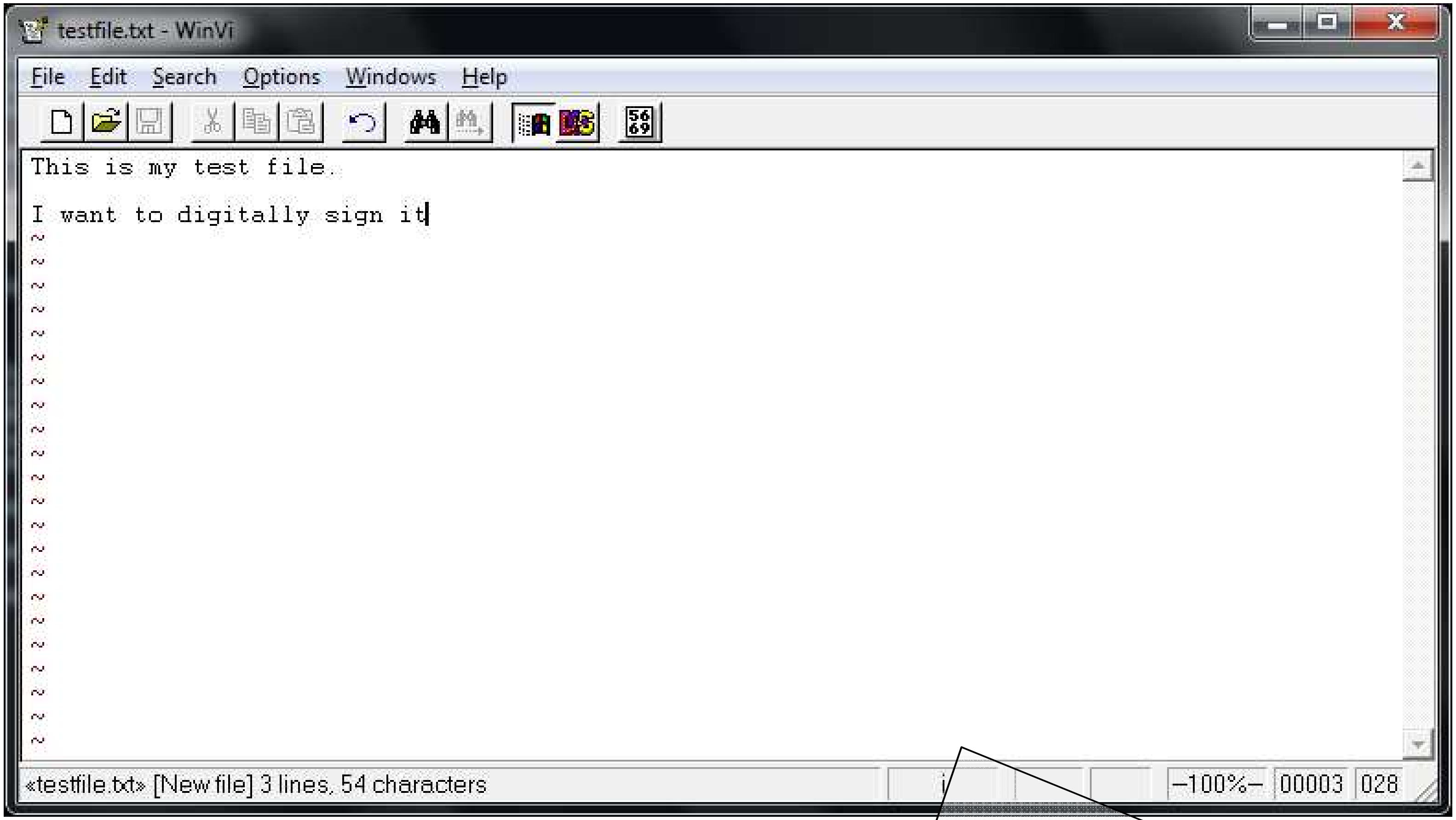
②After receiving a public key from your classmate, import it to your Gpg4win (see next slide)

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



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

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

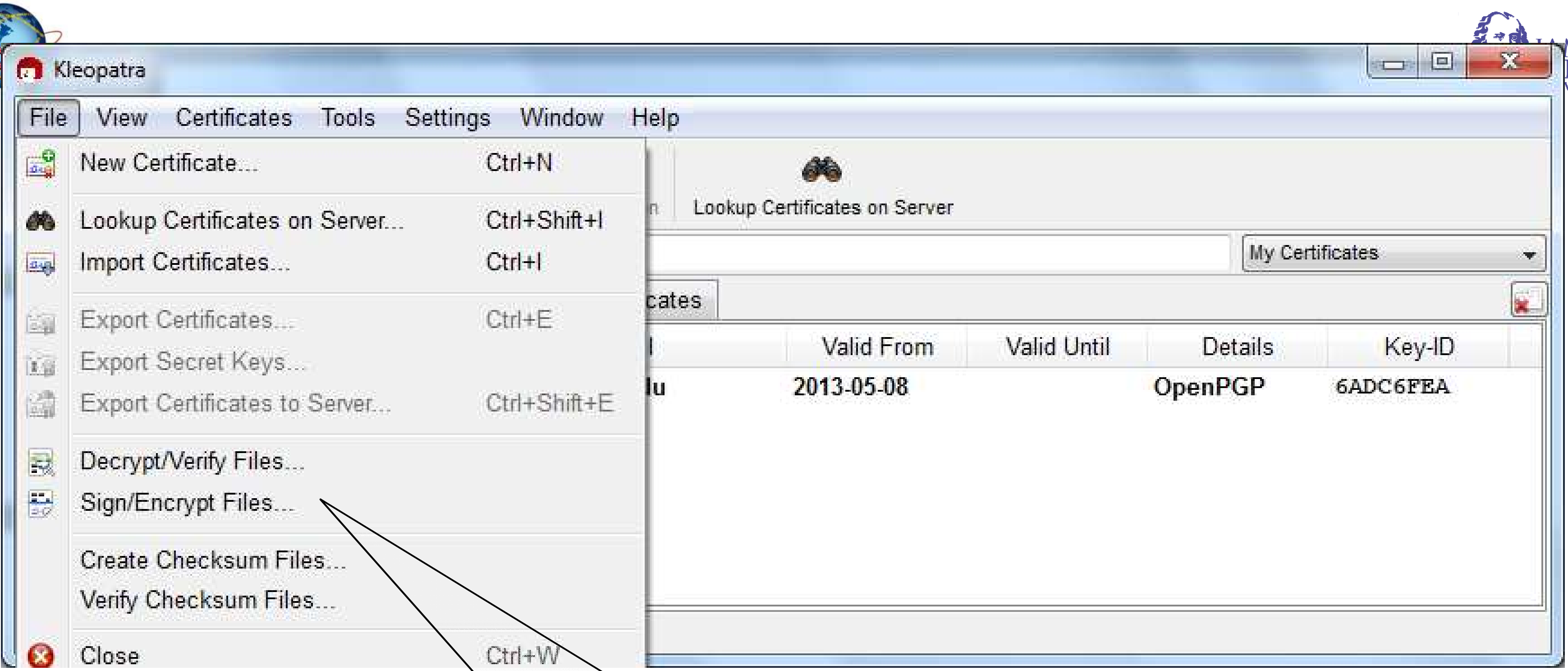


```
This is my test file.

I want to digitally sign it
```

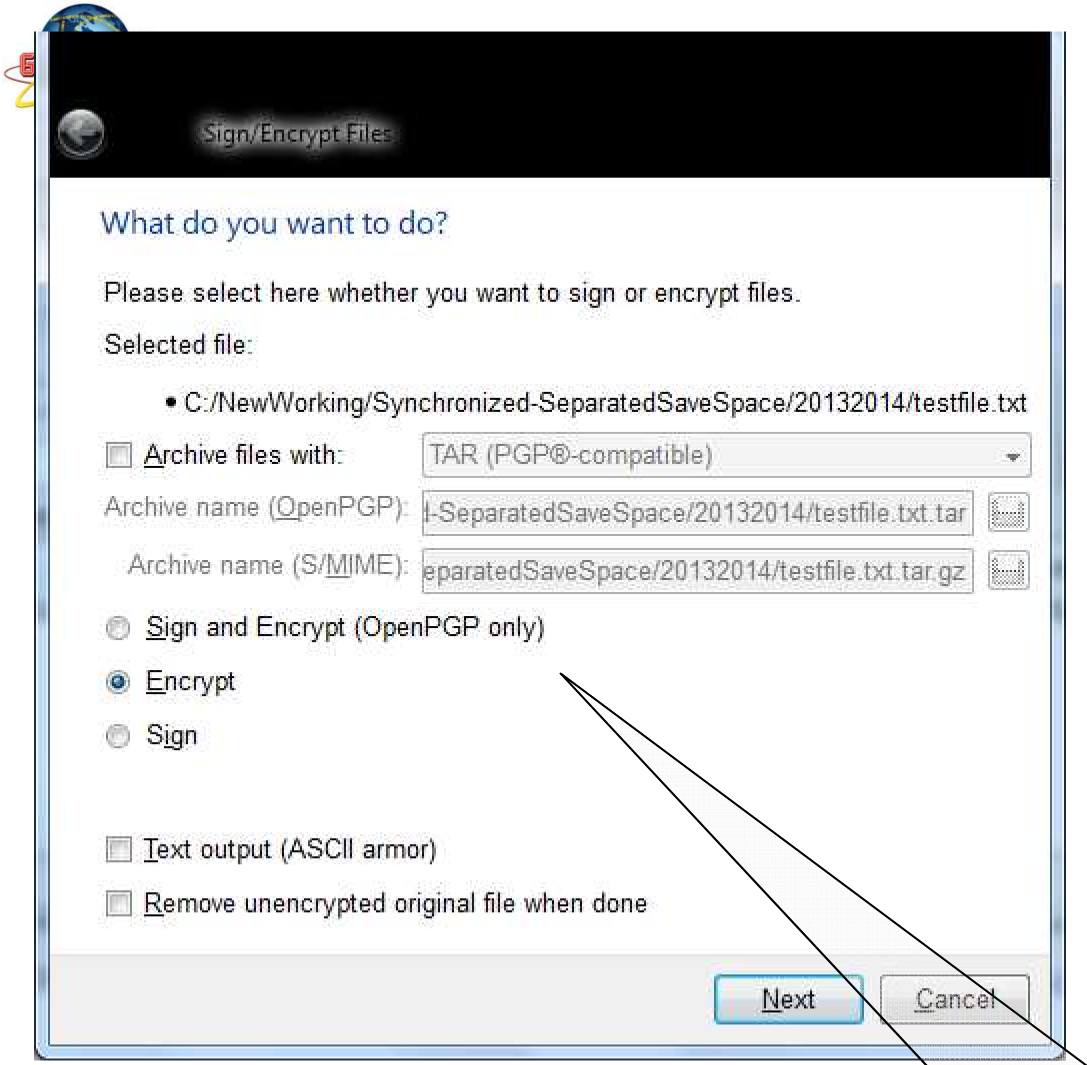
«testfile.txt» [New file] 3 lines, 54 characters —100%— 00003 028

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 ..."



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)

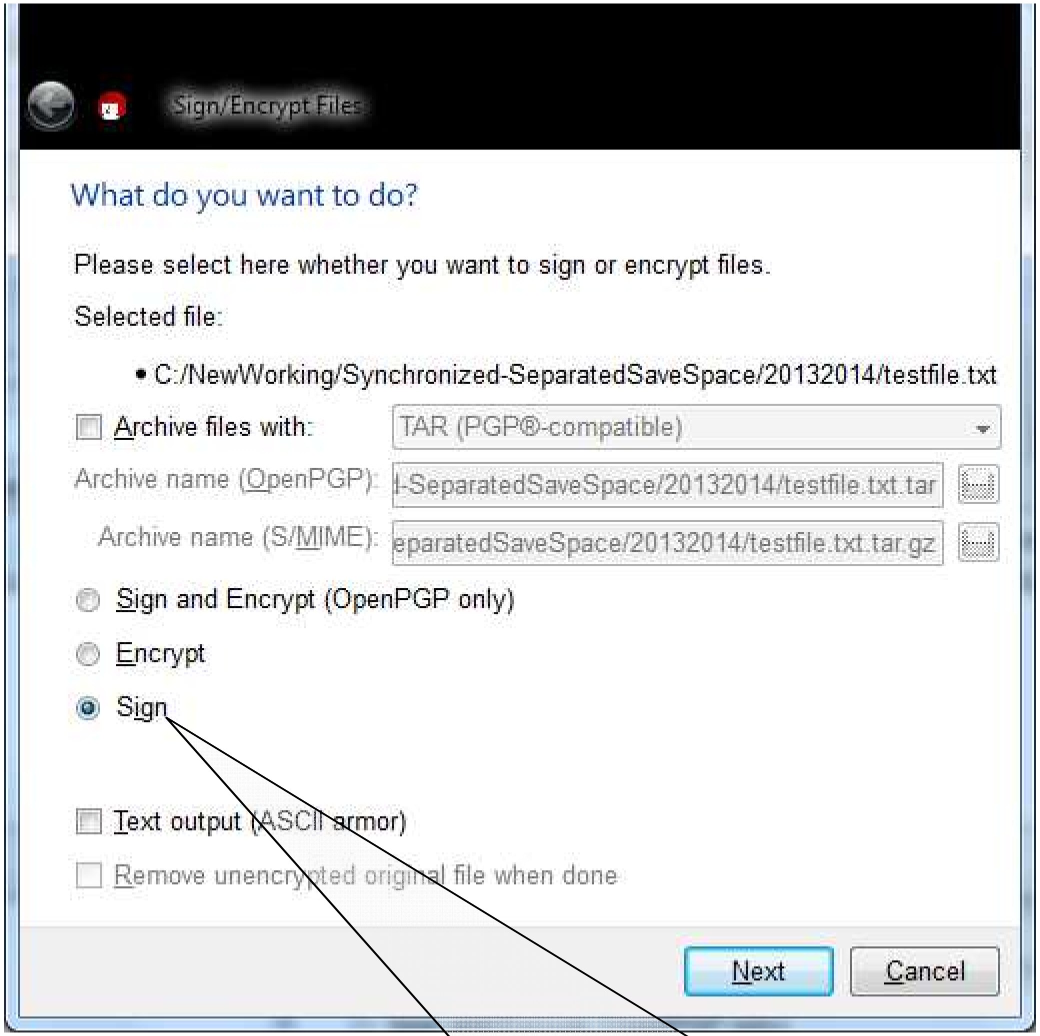
● Encrypt

○ Sign

□ Text output (ASCII armor)

□ Remove unencrypted original file when done

You have three choices



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): -SeparatedSaveSpace/20132014/testfile.txt.tar

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

○ Sign and Encrypt (OpenPGP only)

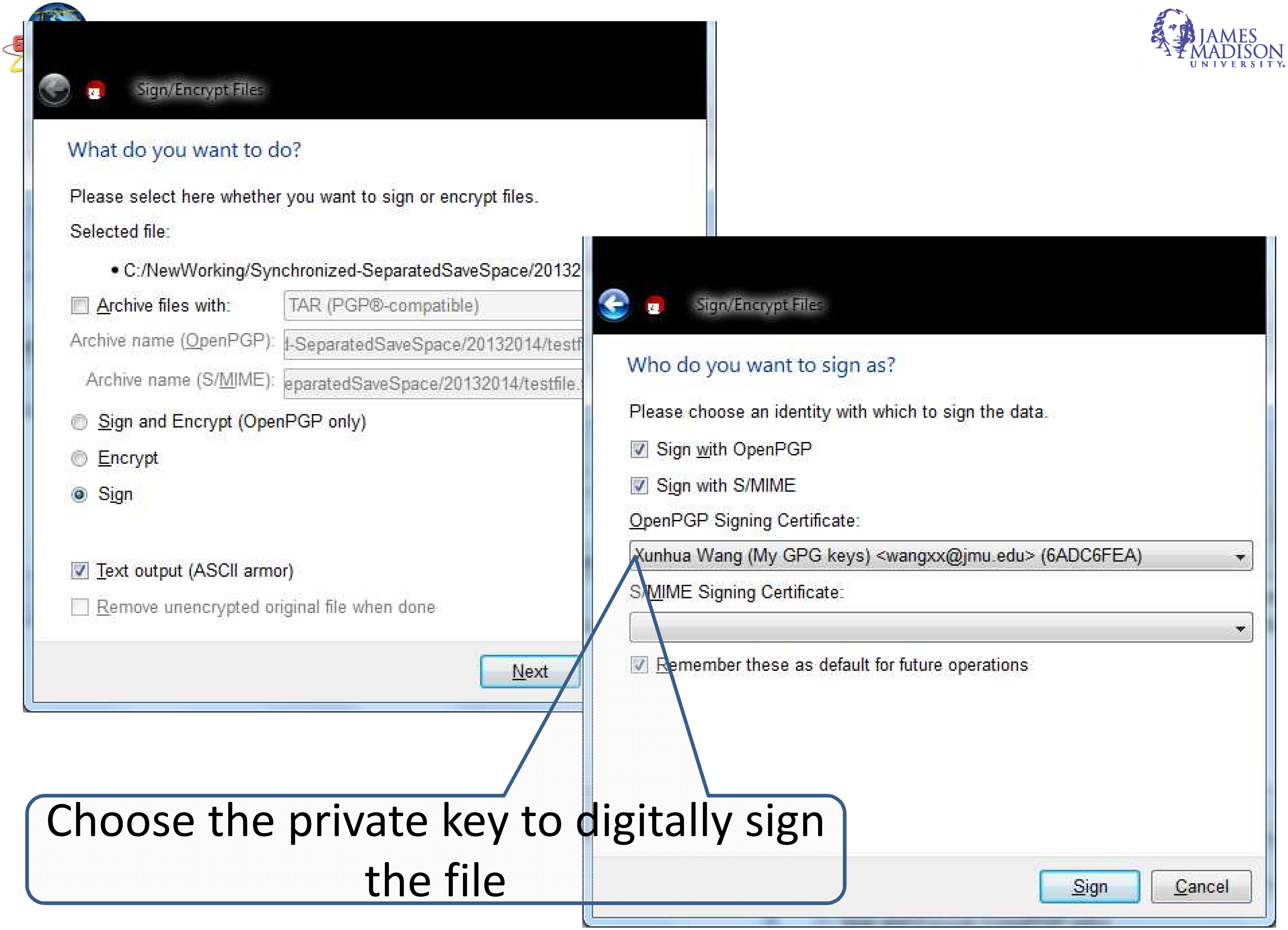
○ Encrypt

● 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

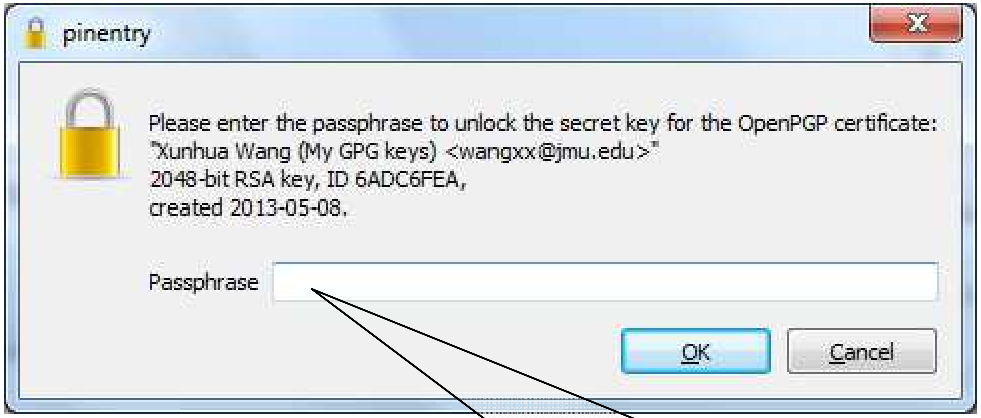
☑ Sign with S/MIME

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

S/MIME Signing Certificate:

☑ Remember these as default for future operations

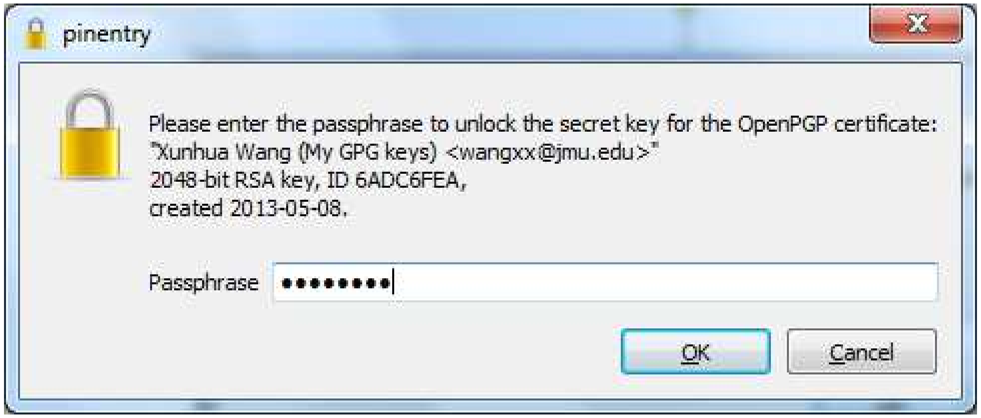
Choose the private key to digitally sign the file



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.

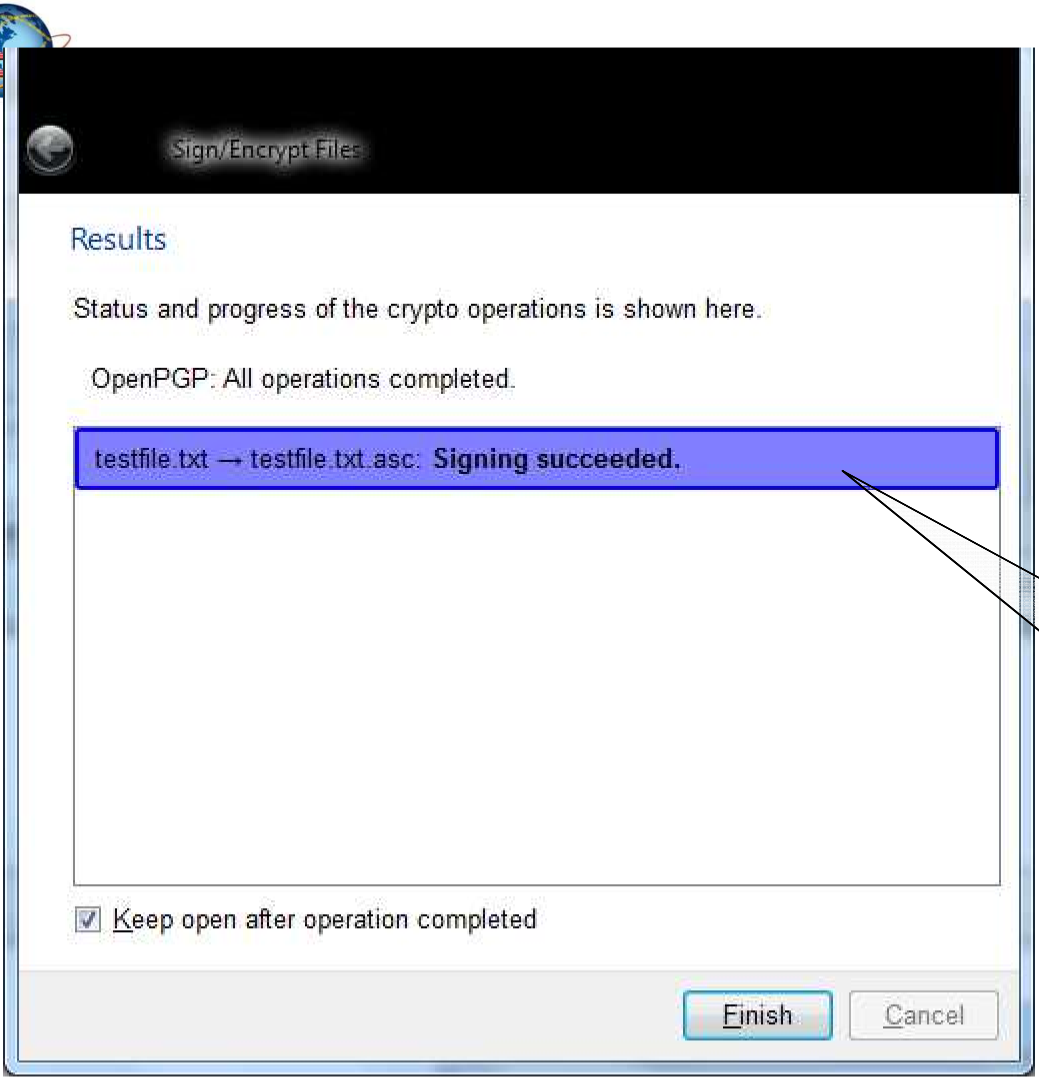
Passphrase

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.

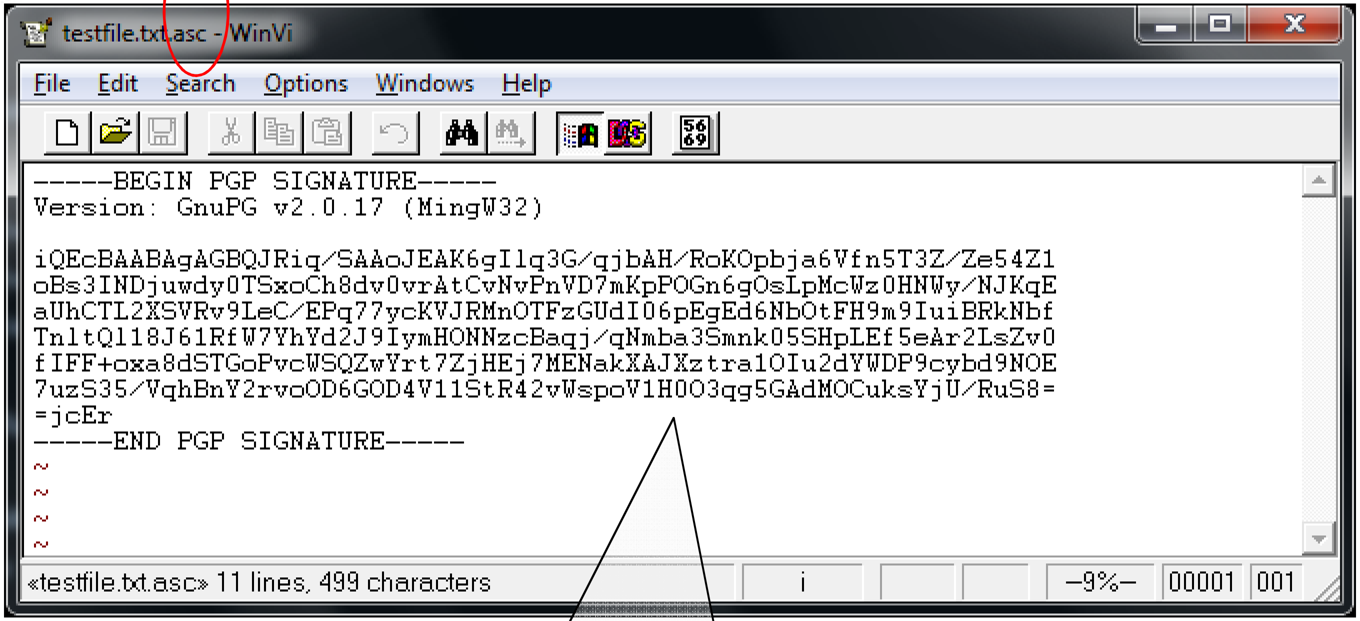
OpenPGP: All operations completed.

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

☑ Keep open after operation completed

Everything is cool

So, where is the digital signature for my file?

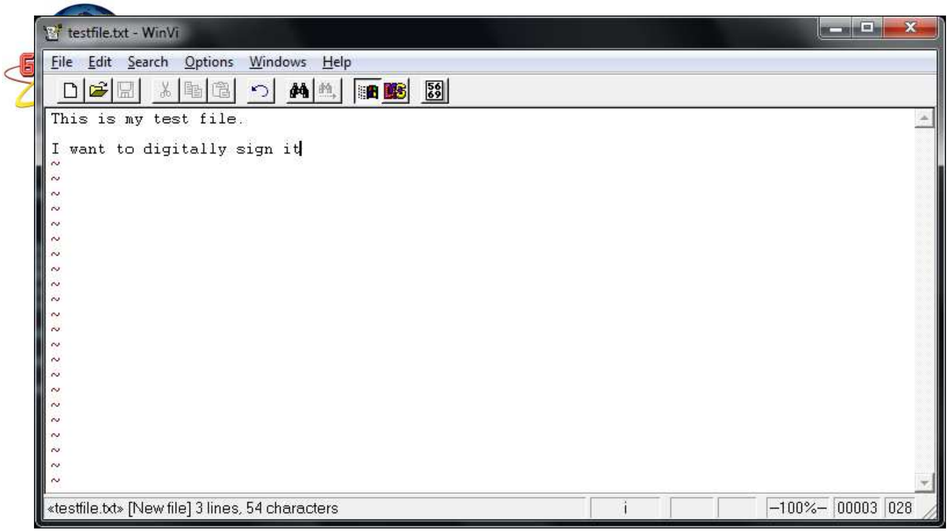


```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.17 (MingW32)

iQEcBAABAgAGBQJRiq/SAAoJEAK6gIlq3G/qjbAH/RoKOpbja6Vfn5T3Z/Ze54Z1
oBs3INDjuwdy0TSxoCh8dv0vrAtCvNvPnVD7mKpPOGn6gOsLpMcWz0HNWy/NJKqE
aUhCTL2XSVRv9LeC/EPq77ycKVJRMnOTFzGUdI06pEgEd6NbOtFH9m9IuiBRkNbf
TnltQl18J61RfW7YhYd2J9IymHONNzcBaqj/qNmba3Smnk05SHpLEf5eAr2LsZv0
fIFF+oxa8dSTGoPvcWSQZwYrt7ZjHEj7MENakXAJXztra1OIu2dYWDP9cybd9NOE
7uzS35/VqhBnY2rvoOD6GOD4V11StR42vWspoV1H0O3qg5GAdMOCuksYjU/RuS8=
=jcEr
-----END PGP SIGNATURE-----
~
~
~
~
```

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

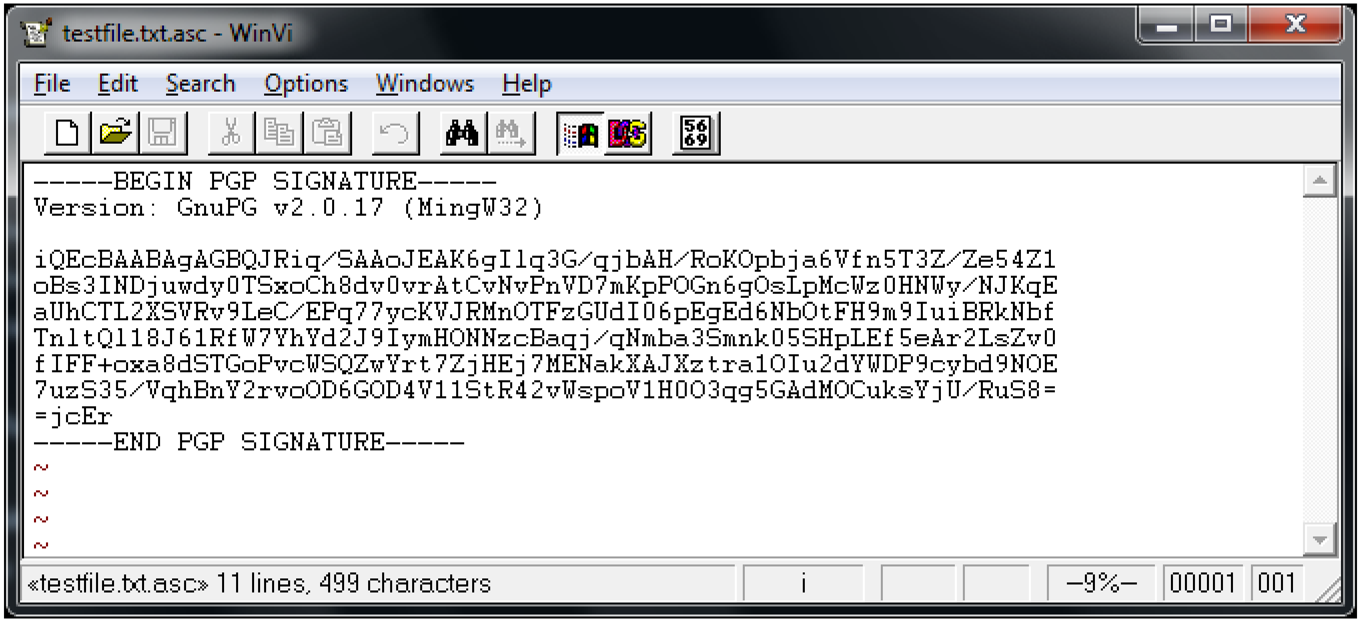
My file is testfile.txt and the signature file is called testfile.txt.asc



```
This is my test file.

I want to digitally sign it
```

«testfile.txt» [New file] 3 lines, 54 characters

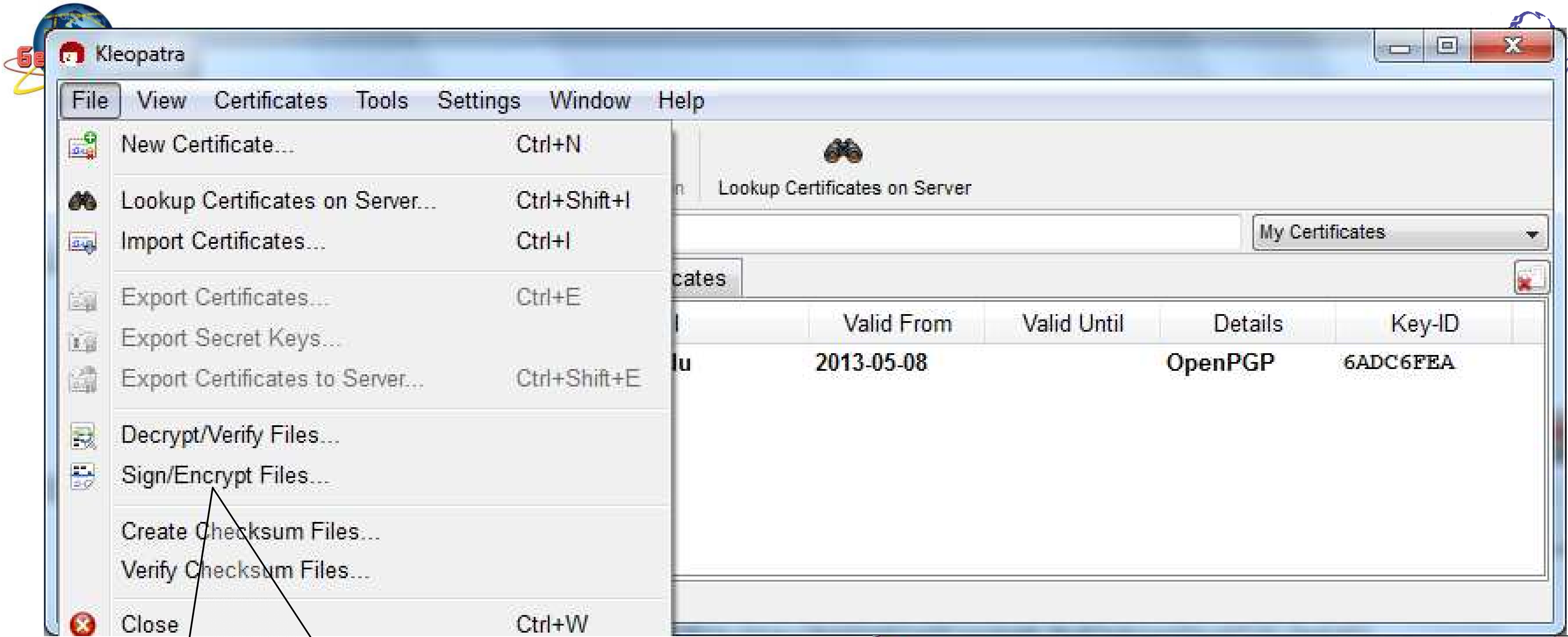


```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.0.17 (MingW32)

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

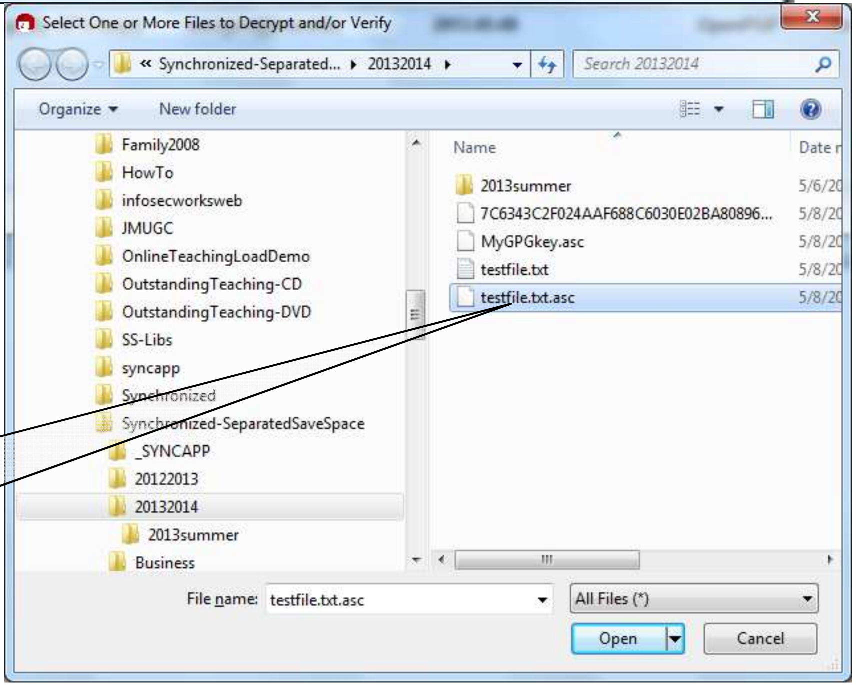
«testfile.txt.asc» 11 lines, 499 characters

Next, I email both my file **and** 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
cates

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

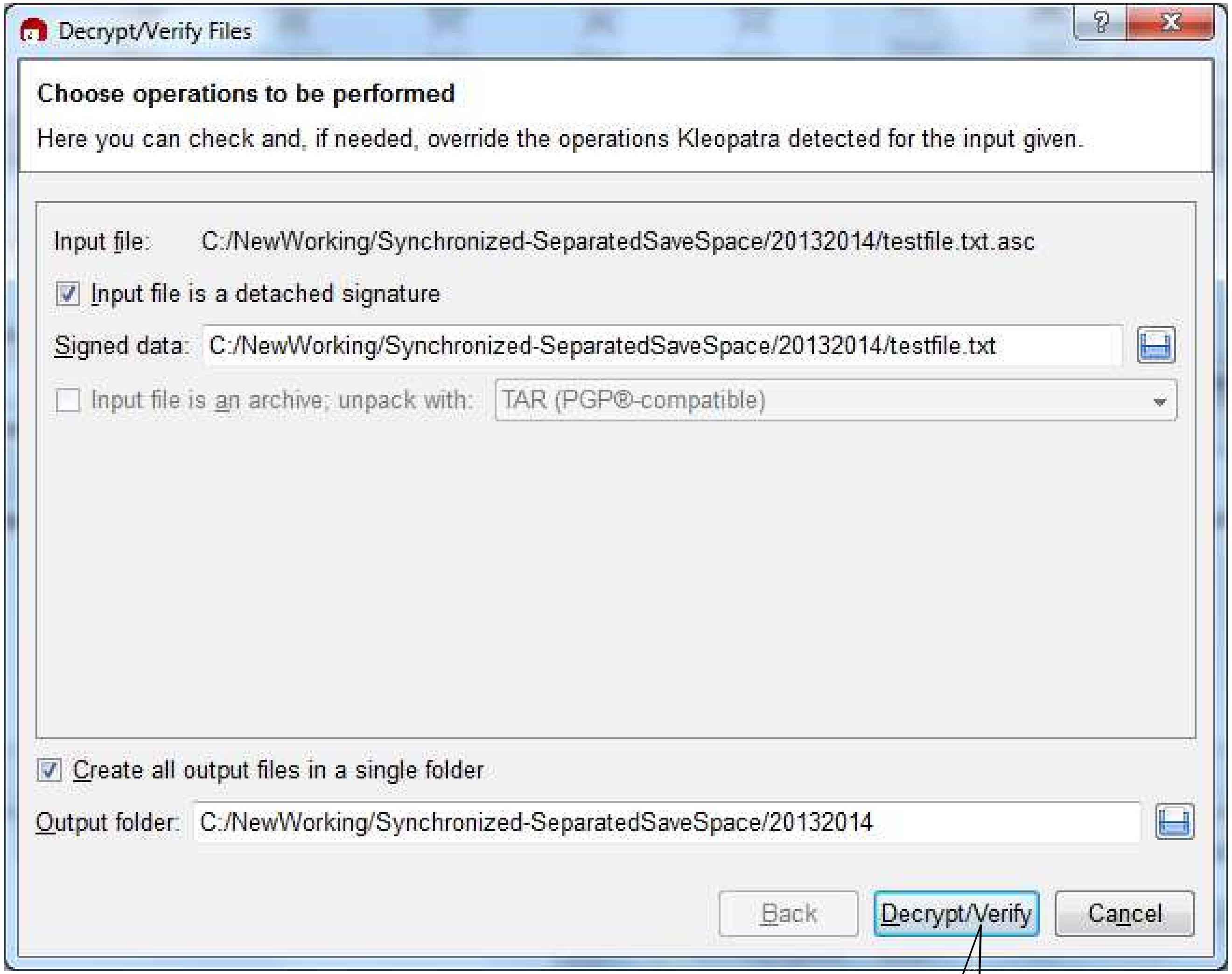
Bob: Click “File -> Decrypt/Verify Files …”



Name	Date m
2013summer	5/6/20
7C6343C2F024AAF688C6030E02BA80896...	5/8/20
MyGPGkey.asc	5/8/20
testfile.txt	5/8/20
testfile.txt.asc	5/8/20

File name: testfile.txt.asc

Bob selects the signature file received from me



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

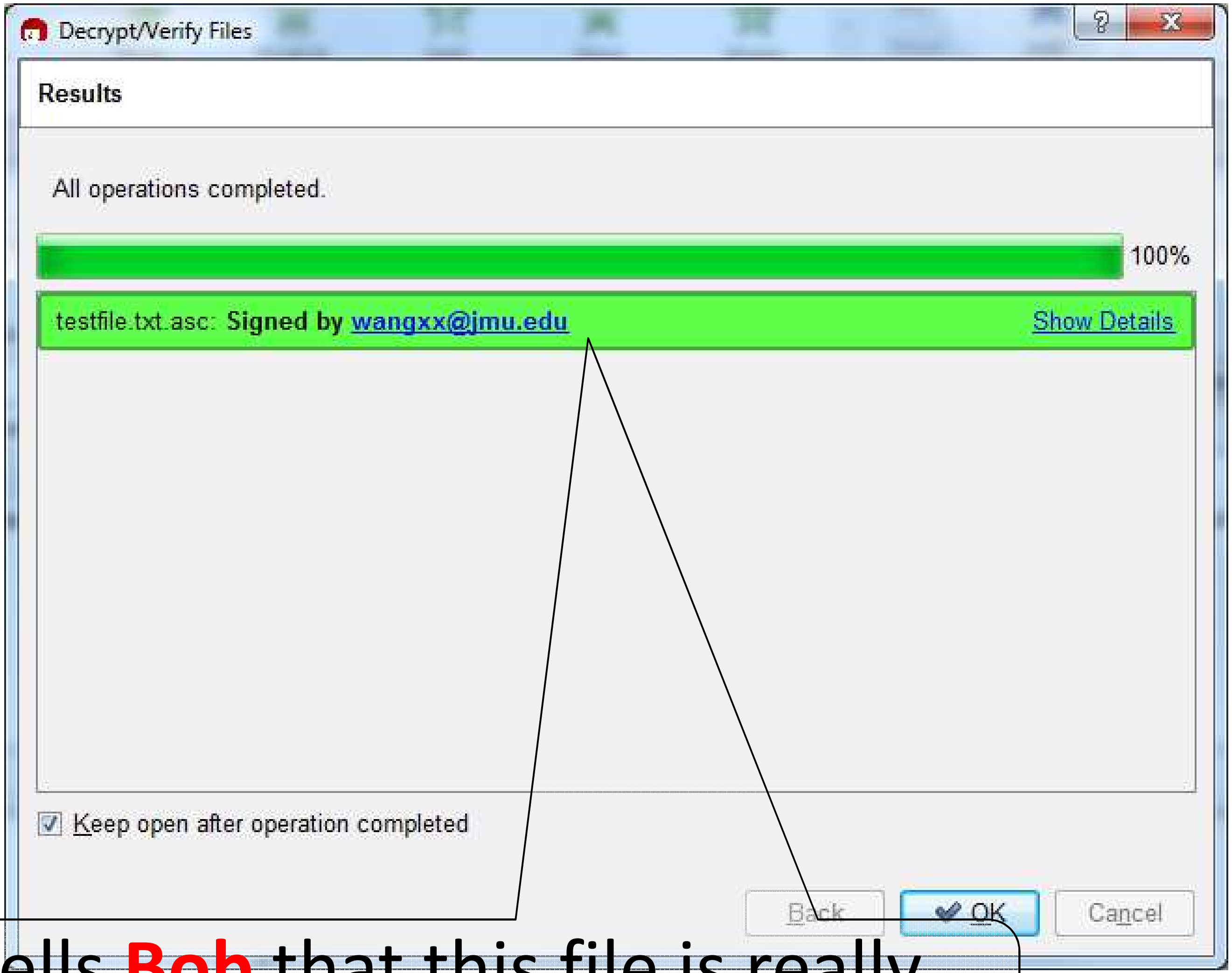
Signed data: C:/NewWorking/Synchronized-SeparatedSaveSpace/20132014/testfile.txt

☐ 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 Show Details

☑ Keep open after operation completed

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

Exercise #2 (2/2)

③Create a text file *your_first_name-last_name-gpg4win.txt* and digitally sign it

④Email *your_first_name-last_name-gpg4win.txt* **and** the digital signature file to your classmate

⑤After 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

Road Map

- Practice
  - ❶Truecrypt
  - ❷GPG
  - ❸BitLocker

BitLocker

- MS Windows has its own driver/disk encryption tool
- BitLocker
  - After Windows 7 Enterprise/Premium
    - Windows 8, 8.1, …
  - Windows 7 professional does not have it

Practice

①If you have a USB drive, you can enable BitLocker on it

– A physical drive

May take an hour to enable BitLocker on a 16G USB drive (one-time operation);

②If you do not have a USB drive, you can create a virtual BitLocker drive

– A virtual drive

Do ① or ②;

② is preferred as it is much faster; jump to slide 81

Practice

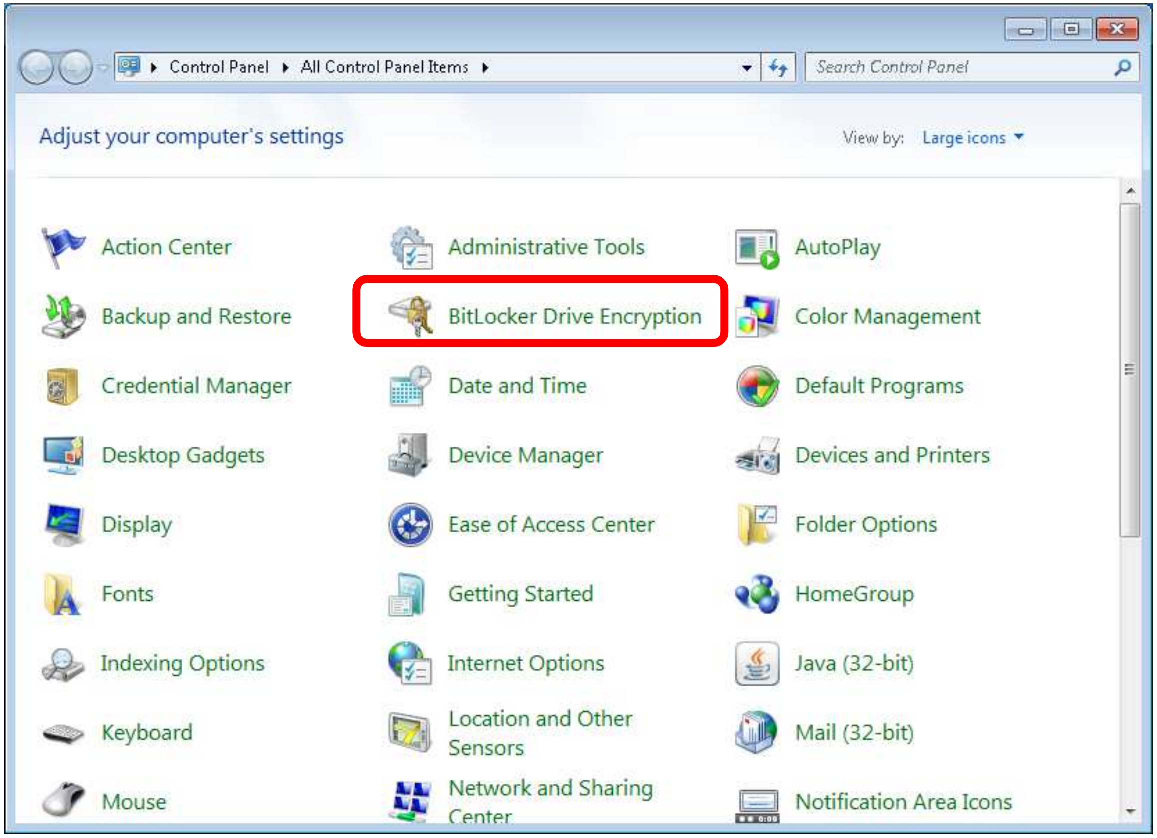
- For this part, do **NOT** use the Windows 2003 virtual machine for previous exercises

- Just use your laptop

For real USB drive only!

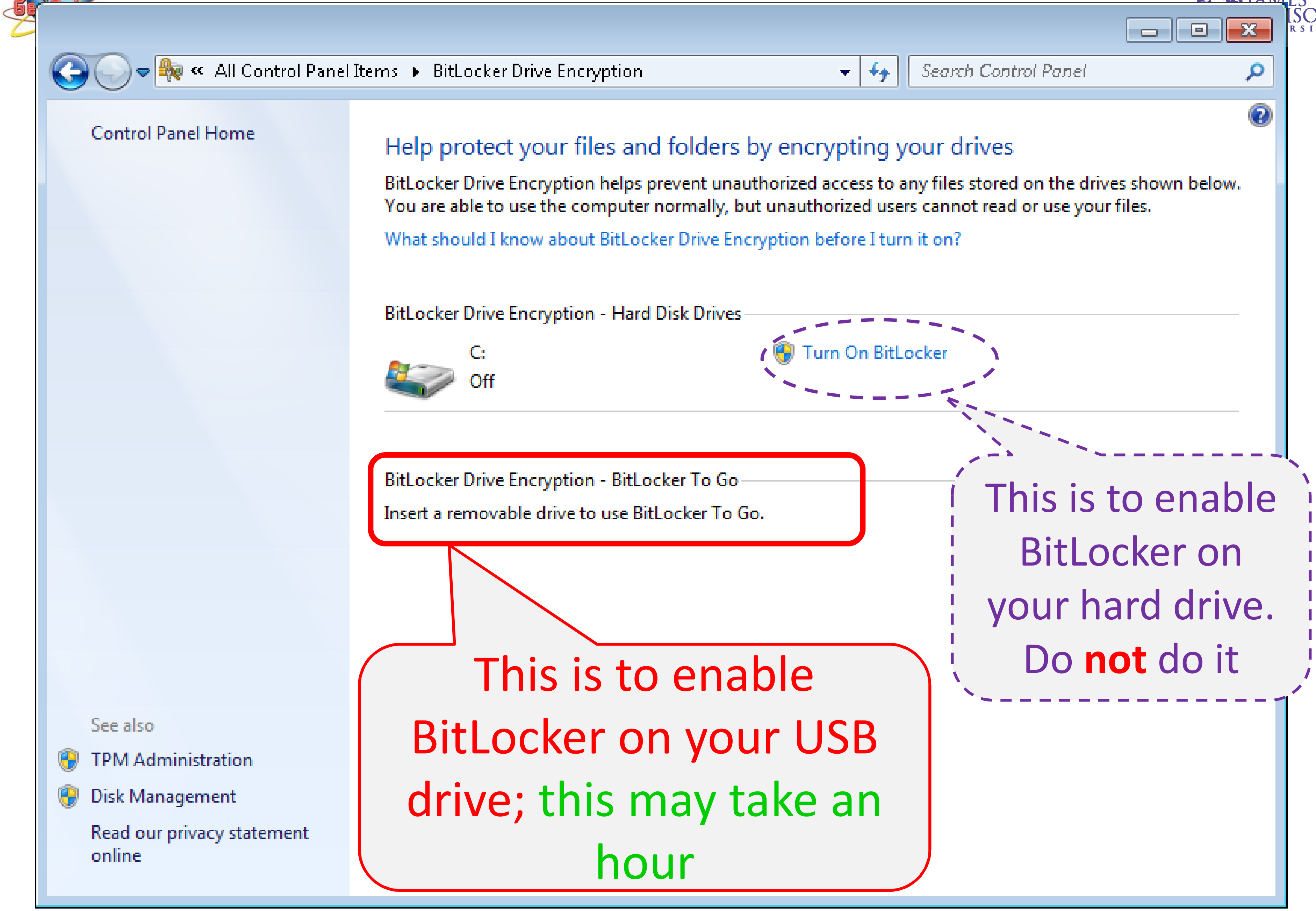
①Enable BitLocker on your USB Drive

- Plug in your USB drive
- Go to “Control Panel”



Adjust your computer's settings

View by: Large icons



Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.

What should I know about BitLocker Drive Encryption before I turn it on?

BitLocker Drive Encryption - Hard Disk Drives

C:
Off

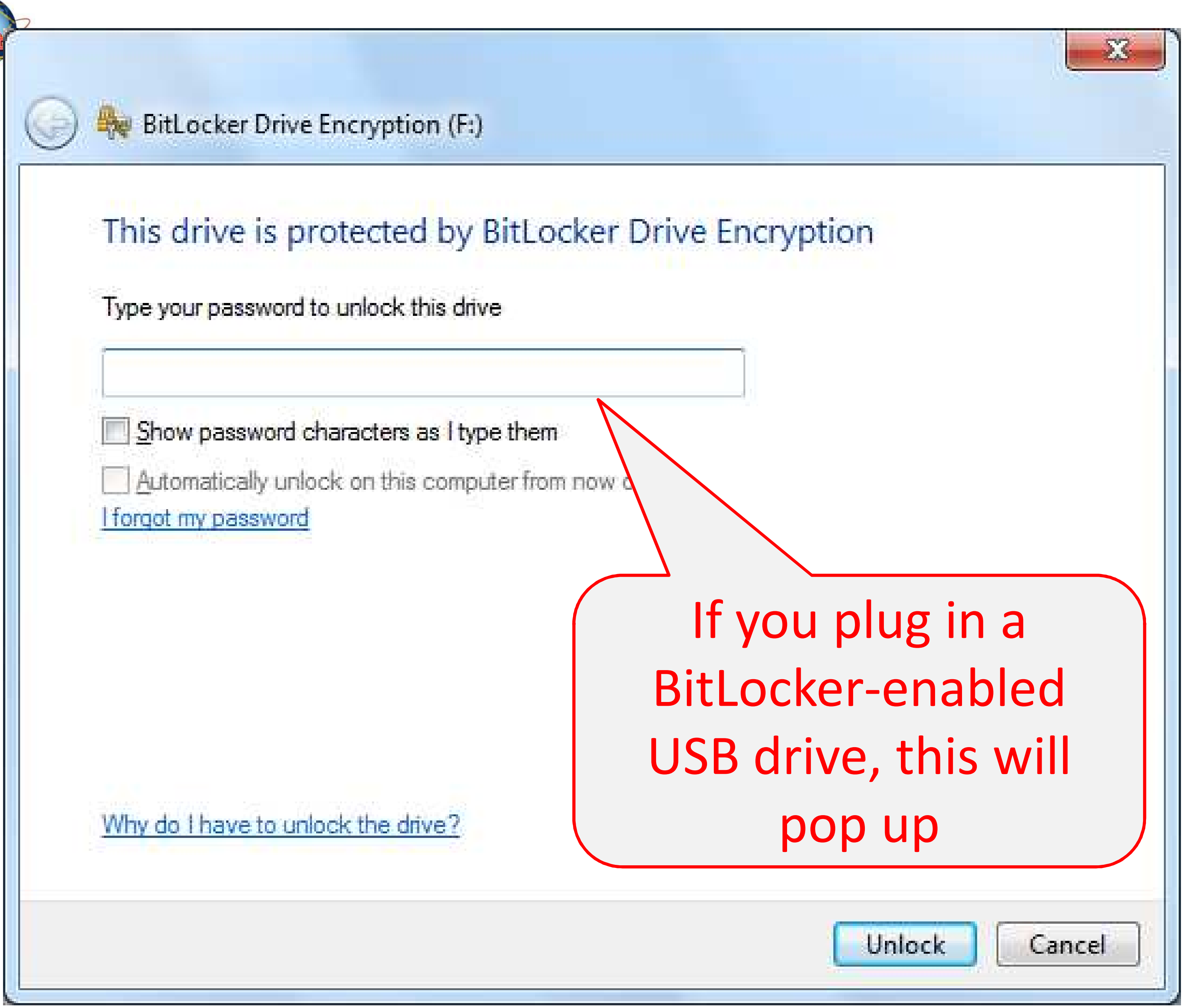
Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go

Insert a removable drive to use BitLocker To Go.

This is to enable BitLocker on your hard drive. Do **not** do it

This is to enable BitLocker on your USB drive; this may take an hour



BitLocker Drive Encryption (F:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

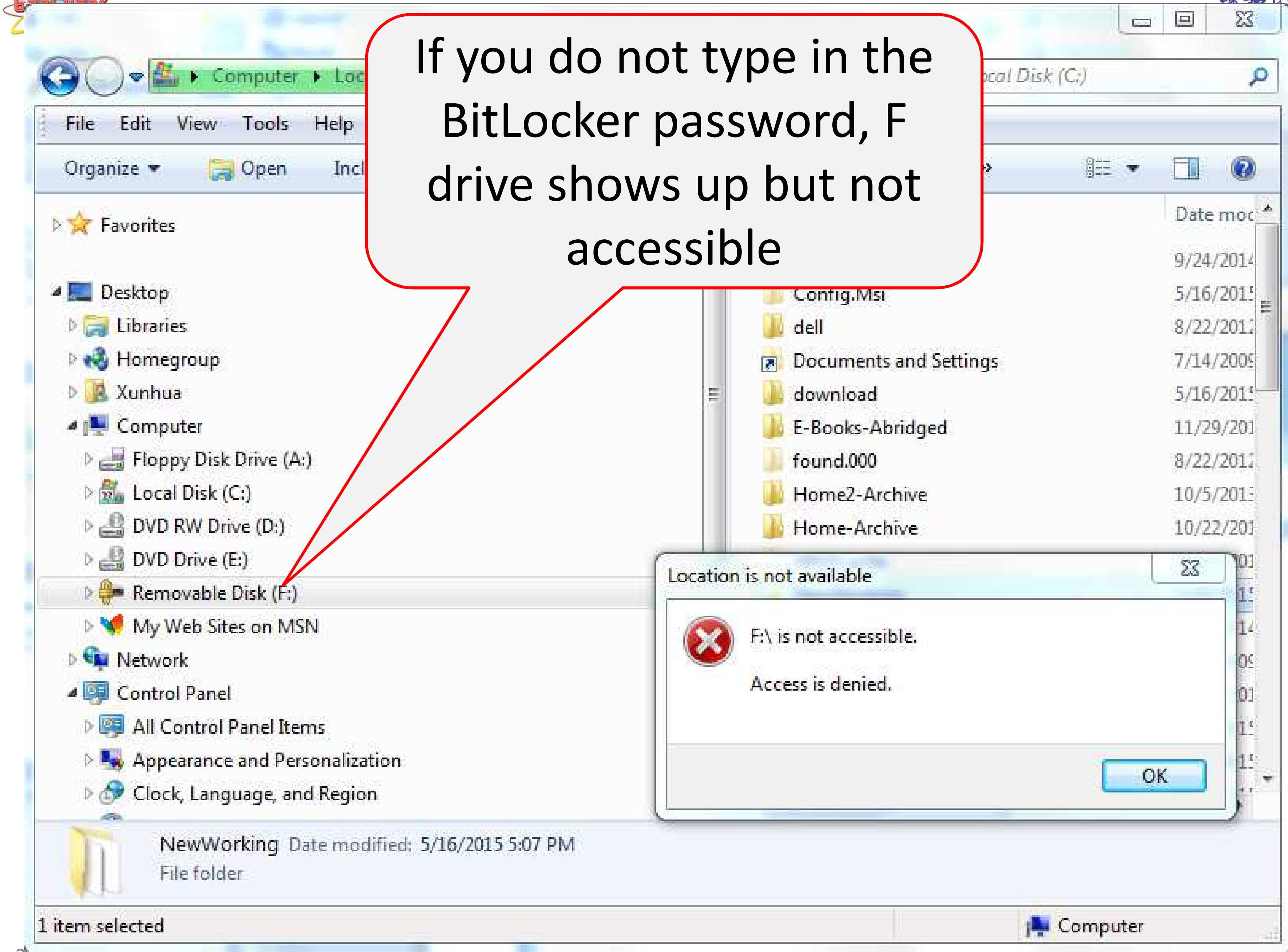
□ Show password characters as I type them

□ Automatically unlock on this computer from now o

I forgot my password

Why do I have to unlock the drive?

If you plug in a BitLocker-enabled USB drive, this will pop up



If you do not type in the BitLocker password, F drive shows up but not accessible

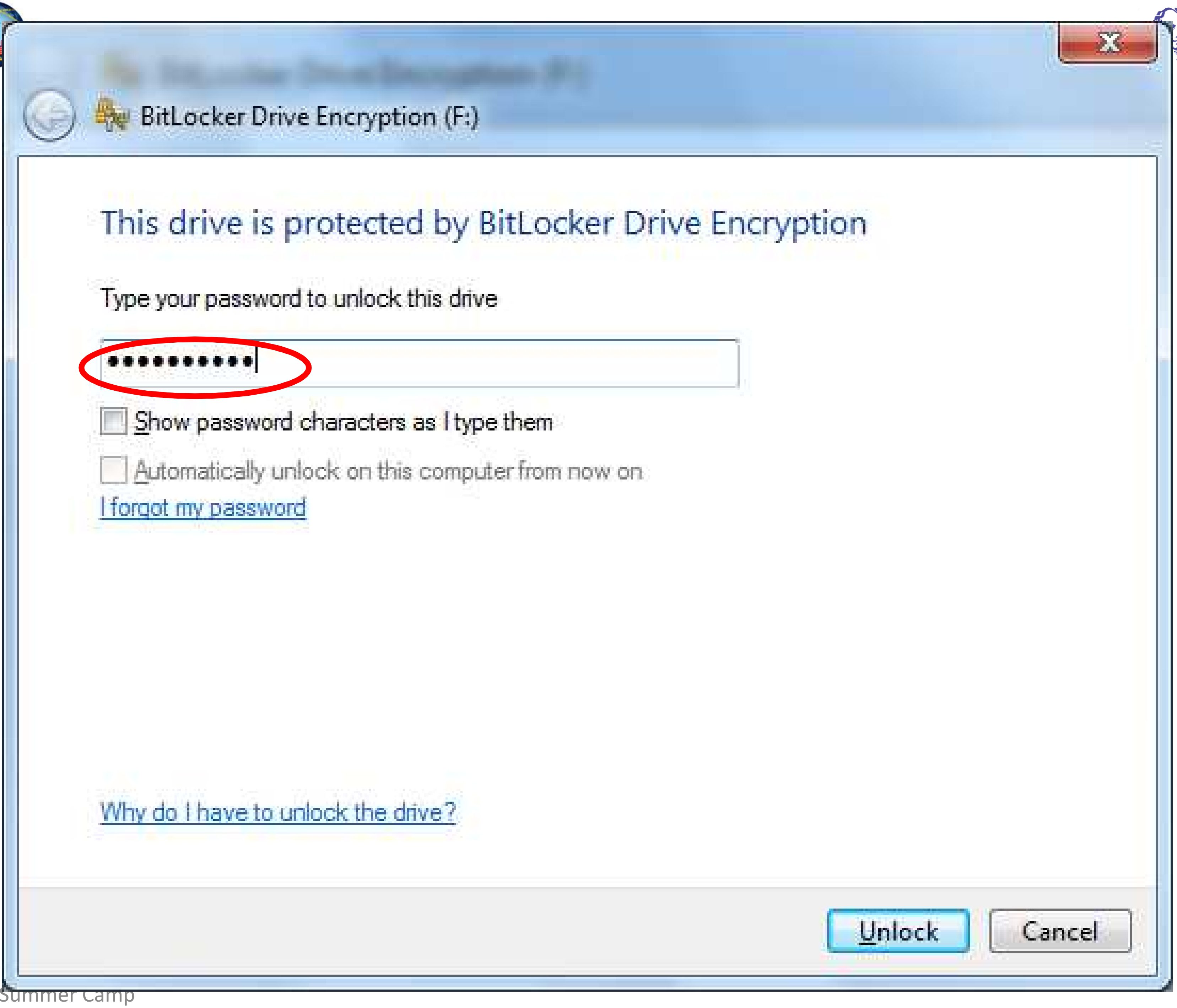
Location is not available

F:\ is not accessible.

Access is denied.

NewWorking Date modified: 5/16/2015 5:07 PM
File folder

1 item selected



BitLocker Drive Encryption (F:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

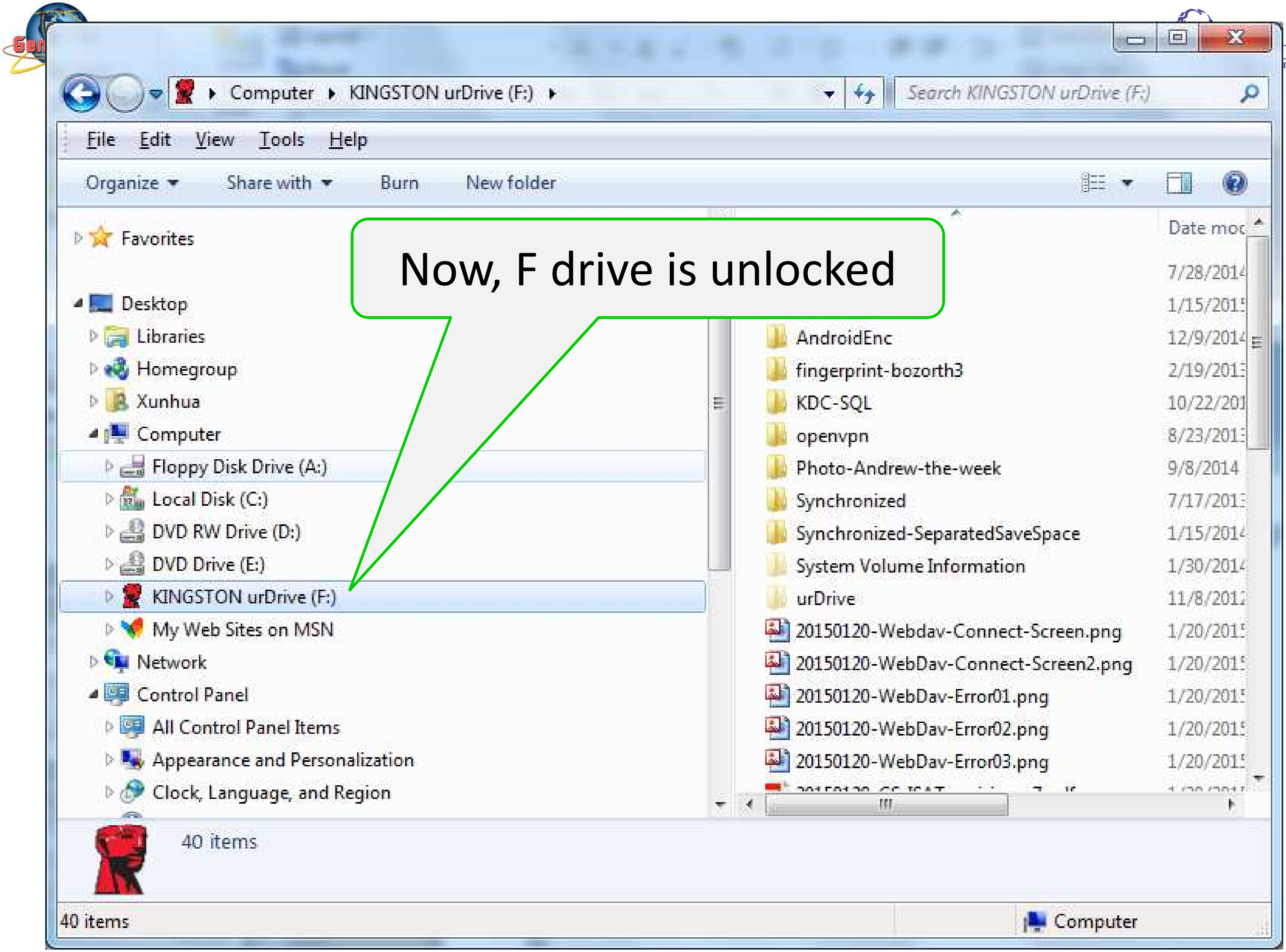
•••••••••••

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?



Now, F drive is unlocked

	Date moc
	7/28/2014
	1/15/2015
AndroidEnc	12/9/2014
fingerprint-bozorth3	2/19/2013
KDC-SQL	10/22/201
openvpn	8/23/2013
Photo-Andrew-the-week	9/8/2014
Synchronized	7/17/2013
Synchronized-SeparatedSaveSpace	1/15/2014
System Volume Information	1/30/2014
urDrive	11/8/2012
20150120-Webdav-Connect-Screen.png	1/20/2015
20150120-WebDav-Connect-Screen2.png	1/20/2015
20150120-WebDav-Error01.png	1/20/2015
20150120-WebDav-Error02.png	1/20/2015
20150120-WebDav-Error03.png	1/20/2015

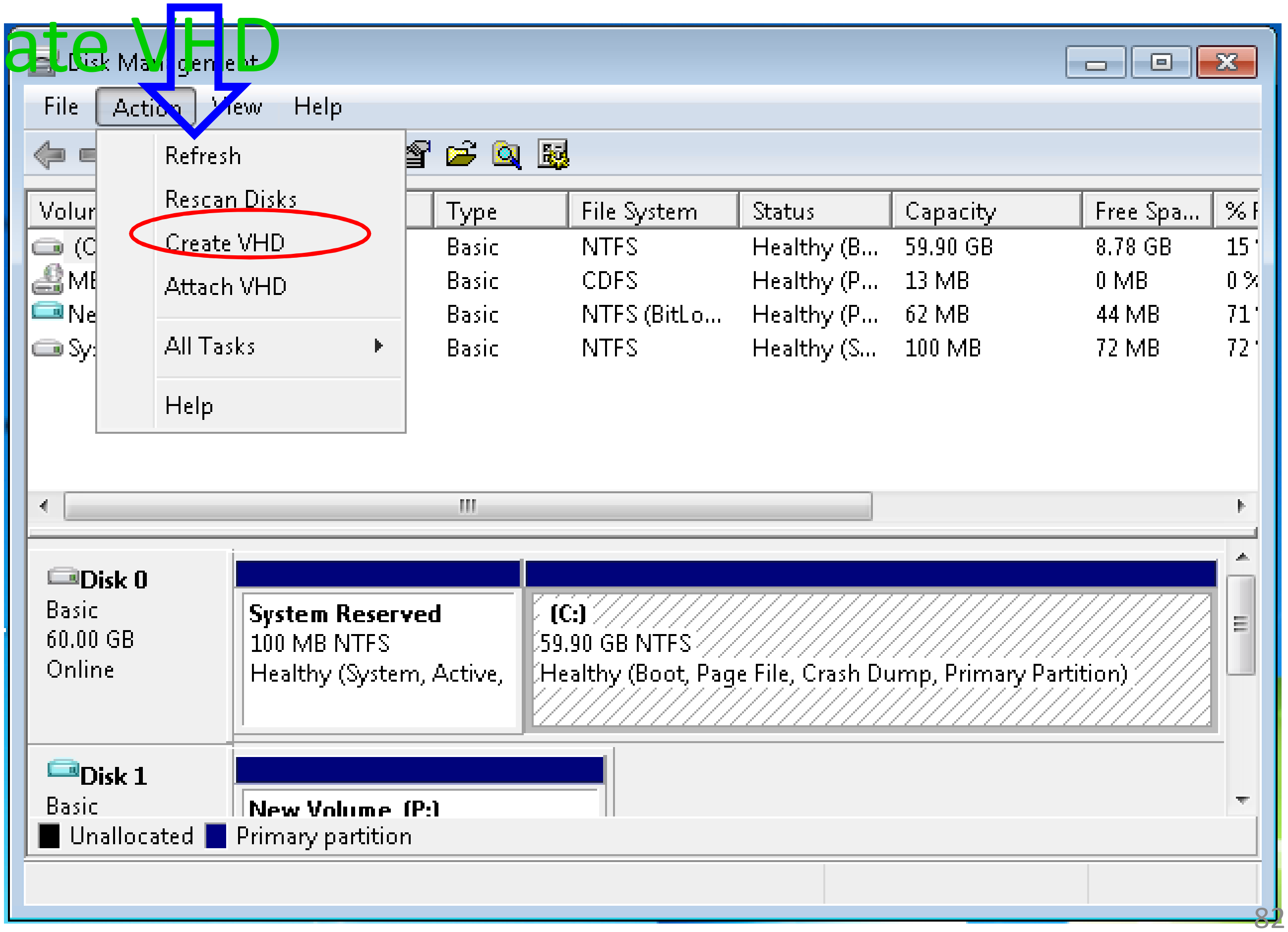
For virtual drive only!

②BitLocker for Virtual Hard Drive File

- General steps
- Create a virtual drive
- Enable BitLocker on it
- Dismount it
- Remount it
  - Copy files to/from it
- Dismount it again

②BitLocker for Virtual Hard Drive File

- On your laptop: diskmgmt.msc
- Action | Create VHD



Volur	Type	File System	Status	Capacity	Free Spa...	% F
(C	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15
ME	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %
Ne	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71
Sy:	Basic	NTFS	Healthy (S...	100 MB	72 MB	72

Disk 0
Basic
60.00 GB
Online

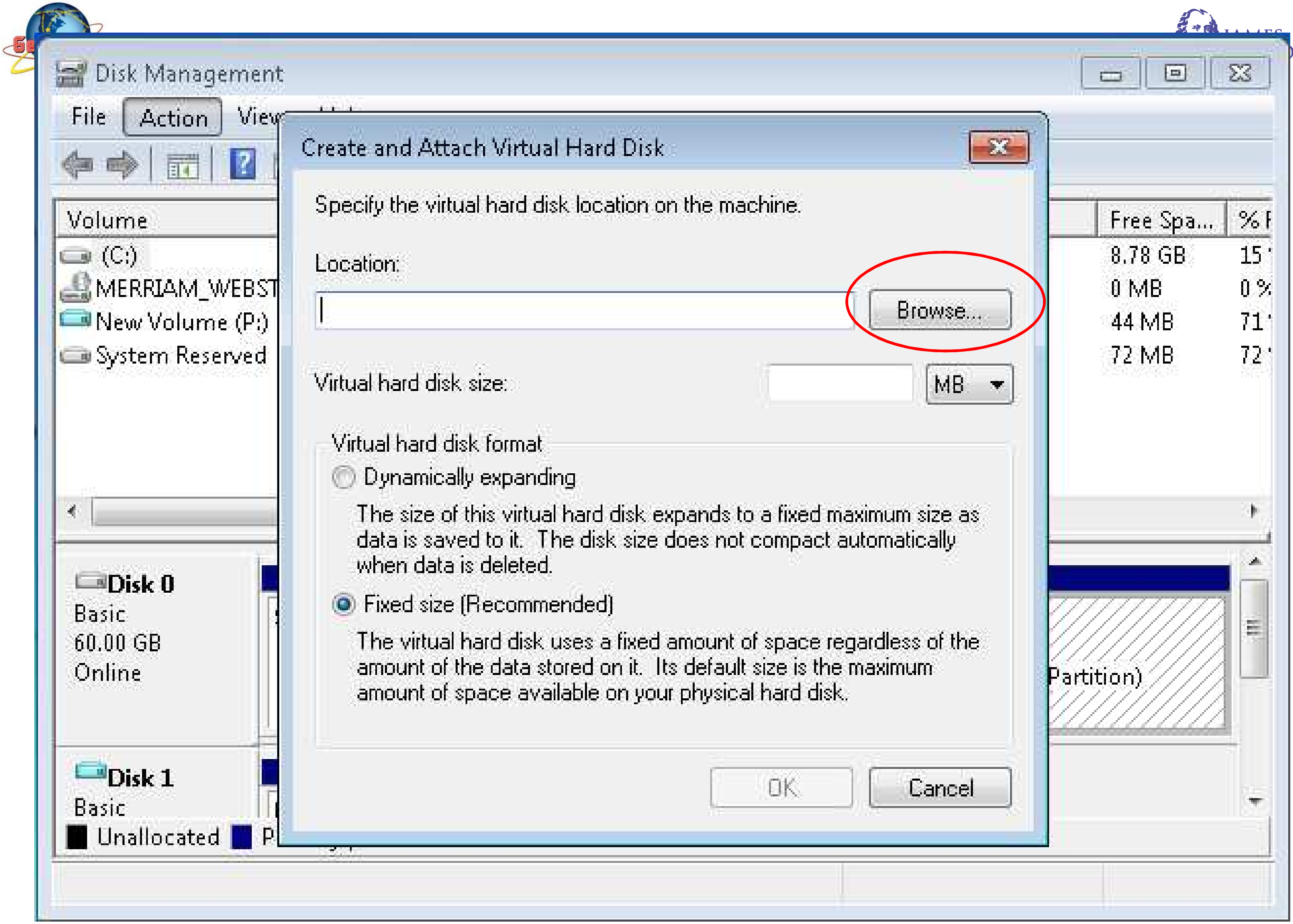
System Reserved
100 MB NTFS
Healthy (System, Active,

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic

New Volume (P:)

■ Unallocated ■ Primary partition



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location:

Browse...

Virtual hard disk size: MB

Virtual hard disk format

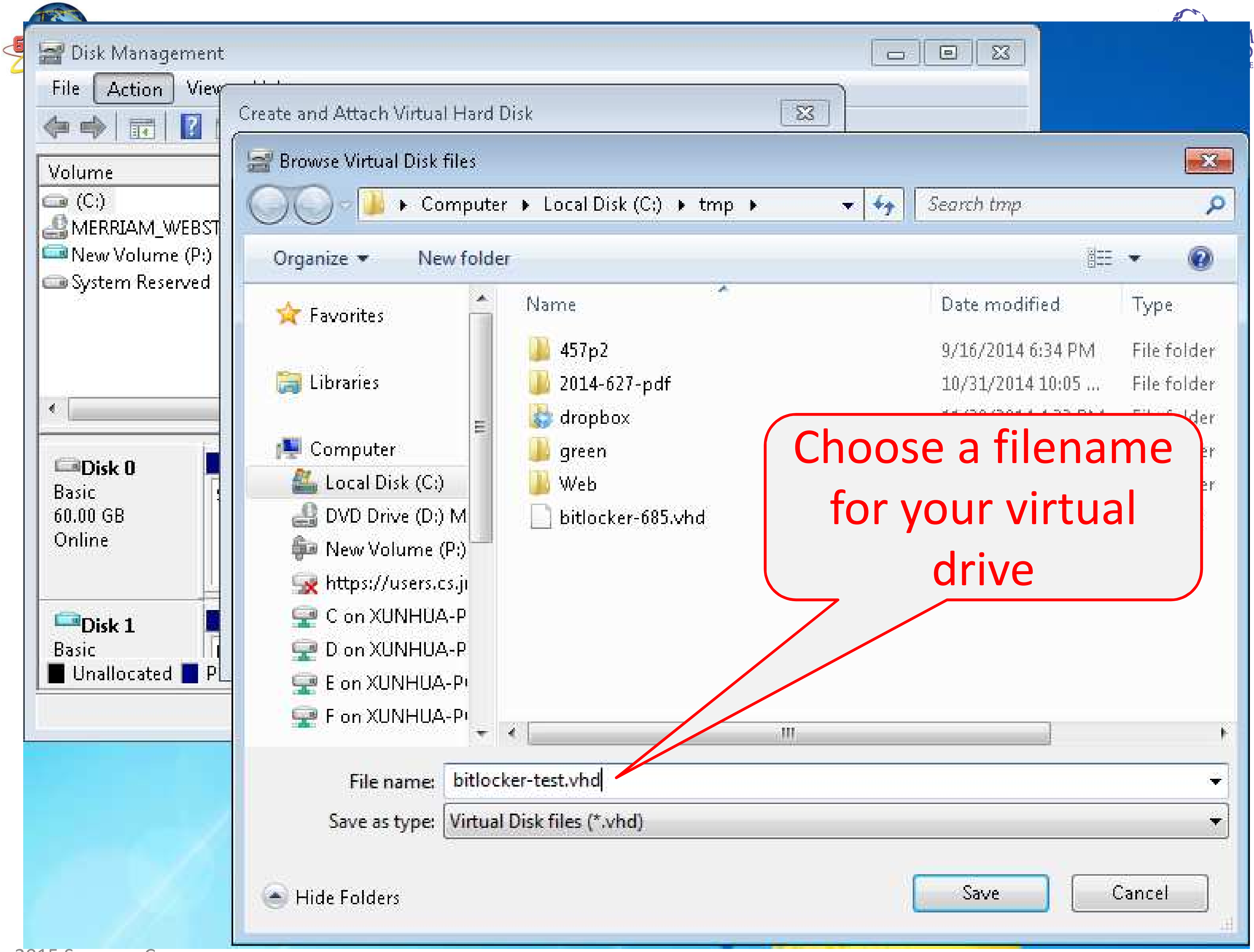
○ Dynamically expanding

The size of this virtual hard disk expands to a fixed maximum size as data is saved to it. The disk size does not compact automatically when data is deleted.

● Fixed size (Recommended)

The virtual hard disk uses a fixed amount of space regardless of the amount of the data stored on it. Its default size is the maximum amount of space available on your physical hard disk.

OK Cancel

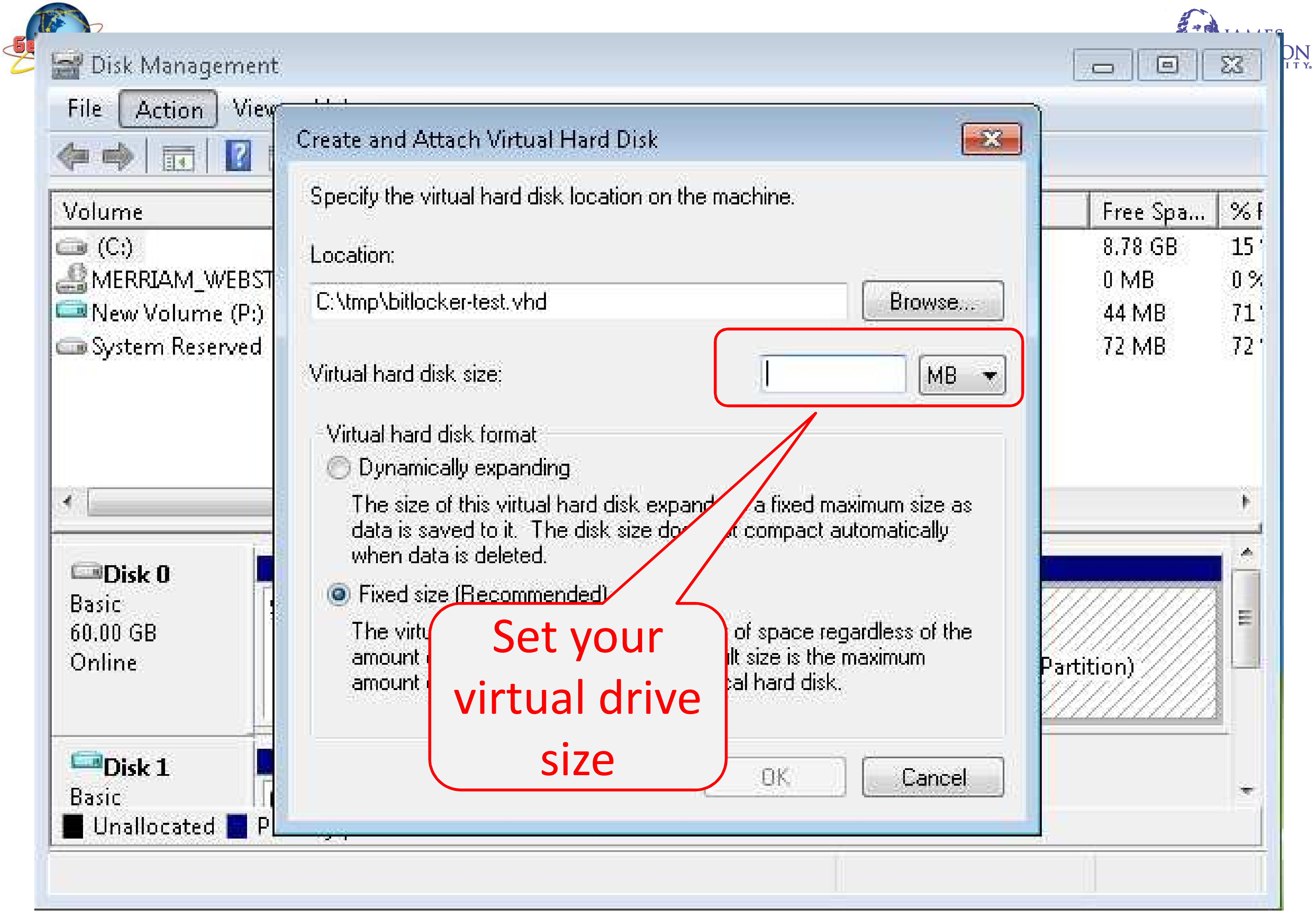


Name	Date modified	Type
457p2	9/16/2014 6:34 PM	File folder
2014-627-pdf	10/31/2014 10:05 ...	File folder
dropbox		
green		
Web		
bitlocker-685.vhd		

File name: bitlocker-test.vhd

Save as type: Virtual Disk files (*.vhd)

Choose a filename for your virtual drive



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location:

C:\tmp\bitlocker-test.vhd

Browse...

Virtual hard disk size: | MB ▾

Virtual hard disk format

○ Dynamically expanding

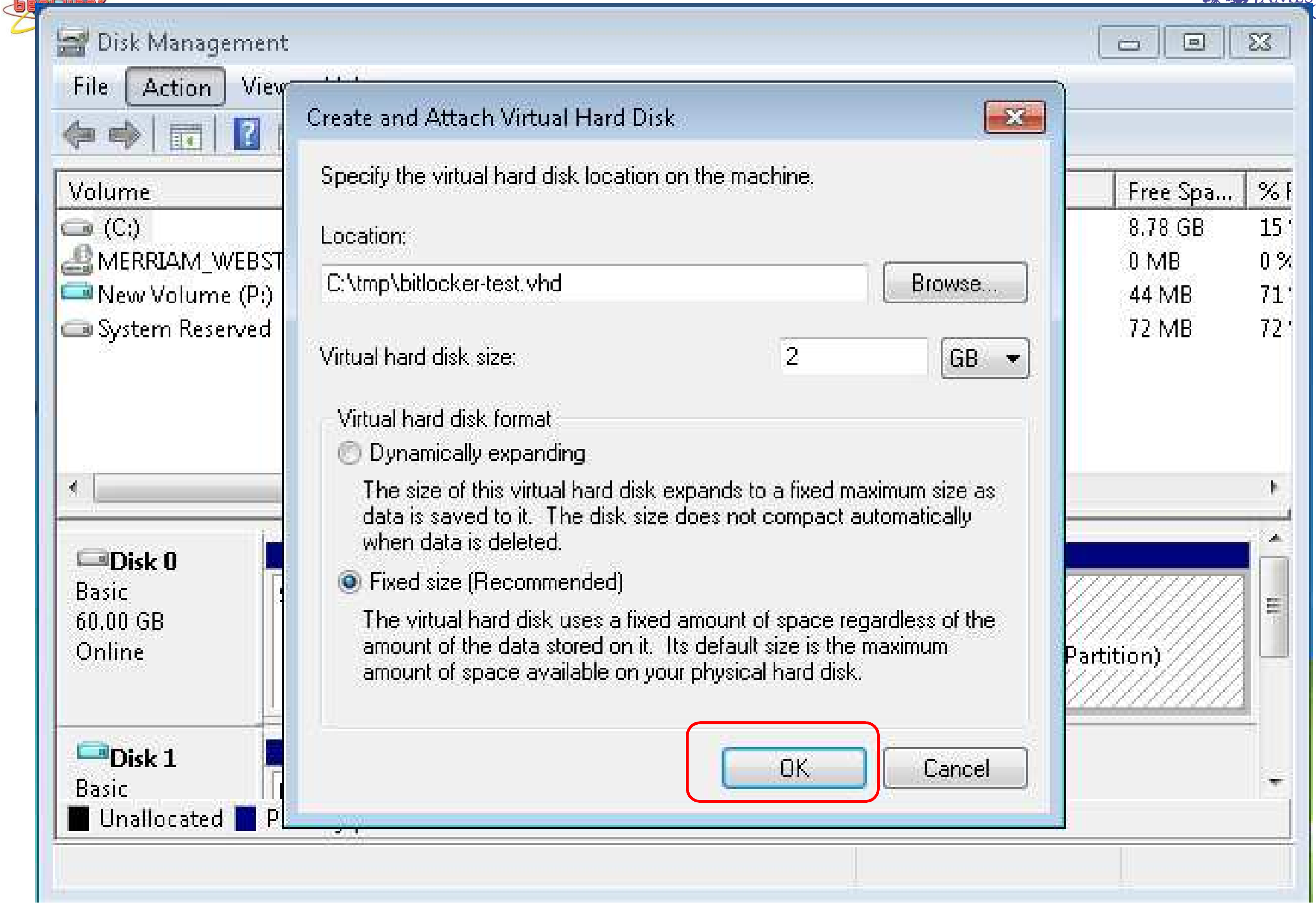
The size of this virtual hard disk expand a fixed maximum size as data is saved to it. The disk size do t compact automatically when data is deleted.

● Fixed size (Recommended)

The virtu of space regardless of the amount lt size is the maximum amount al hard disk.

OK Cancel

Set your virtual drive size



Specify the virtual hard disk location on the machine.

Location: C:\tmp\bitlocker-test.vhd

Virtual hard disk size: 2 GB

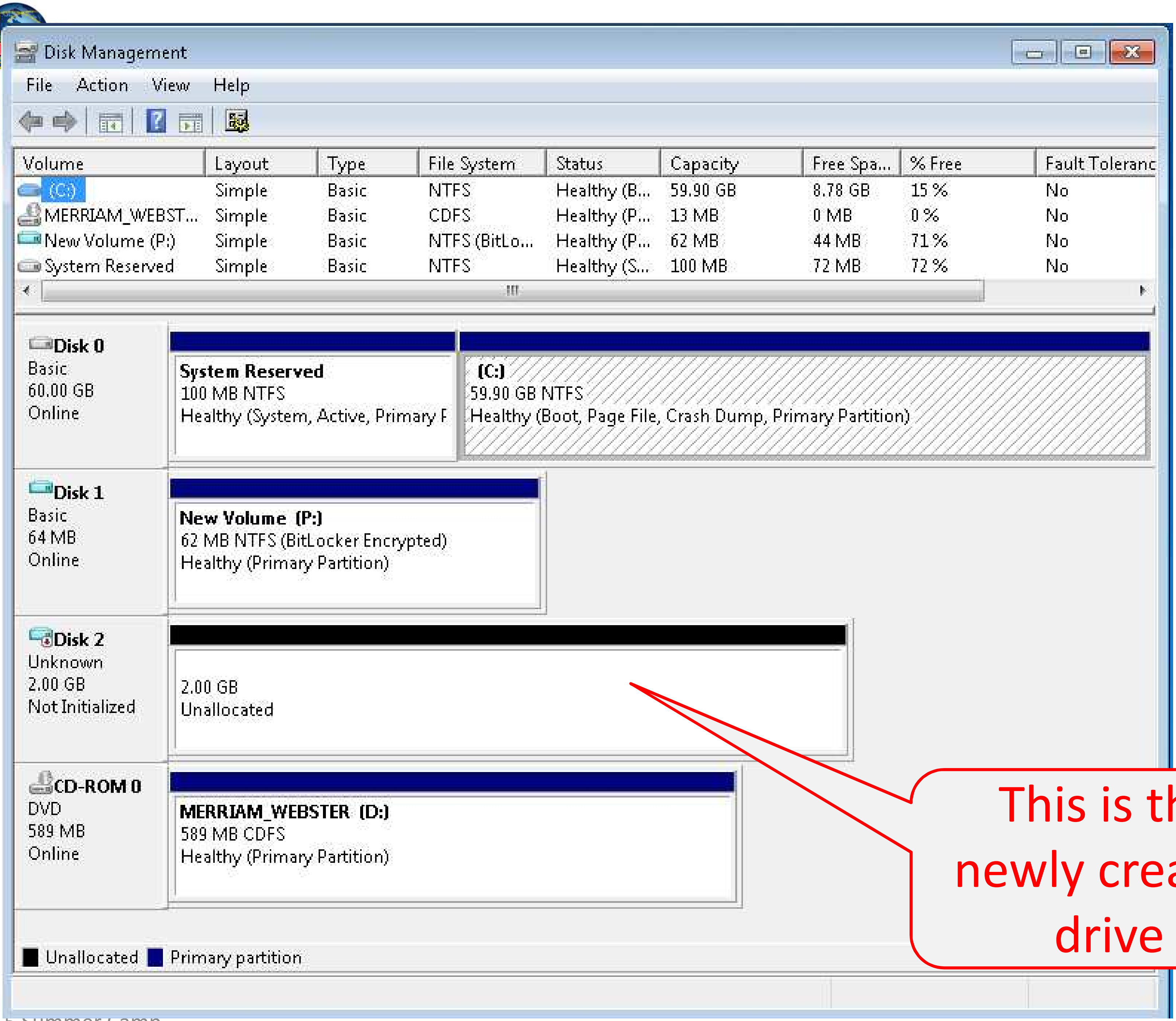
Virtual hard disk format

○ Dynamically expanding

The size of this virtual hard disk expands to a fixed maximum size as data is saved to it. The disk size does not compact automatically when data is deleted.

● Fixed size (Recommended)

The virtual hard disk uses a fixed amount of space regardless of the amount of the data stored on it. Its default size is the maximum amount of space available on your physical hard disk.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	72 MB	72 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Unknown
2.00 GB
Not Initialized

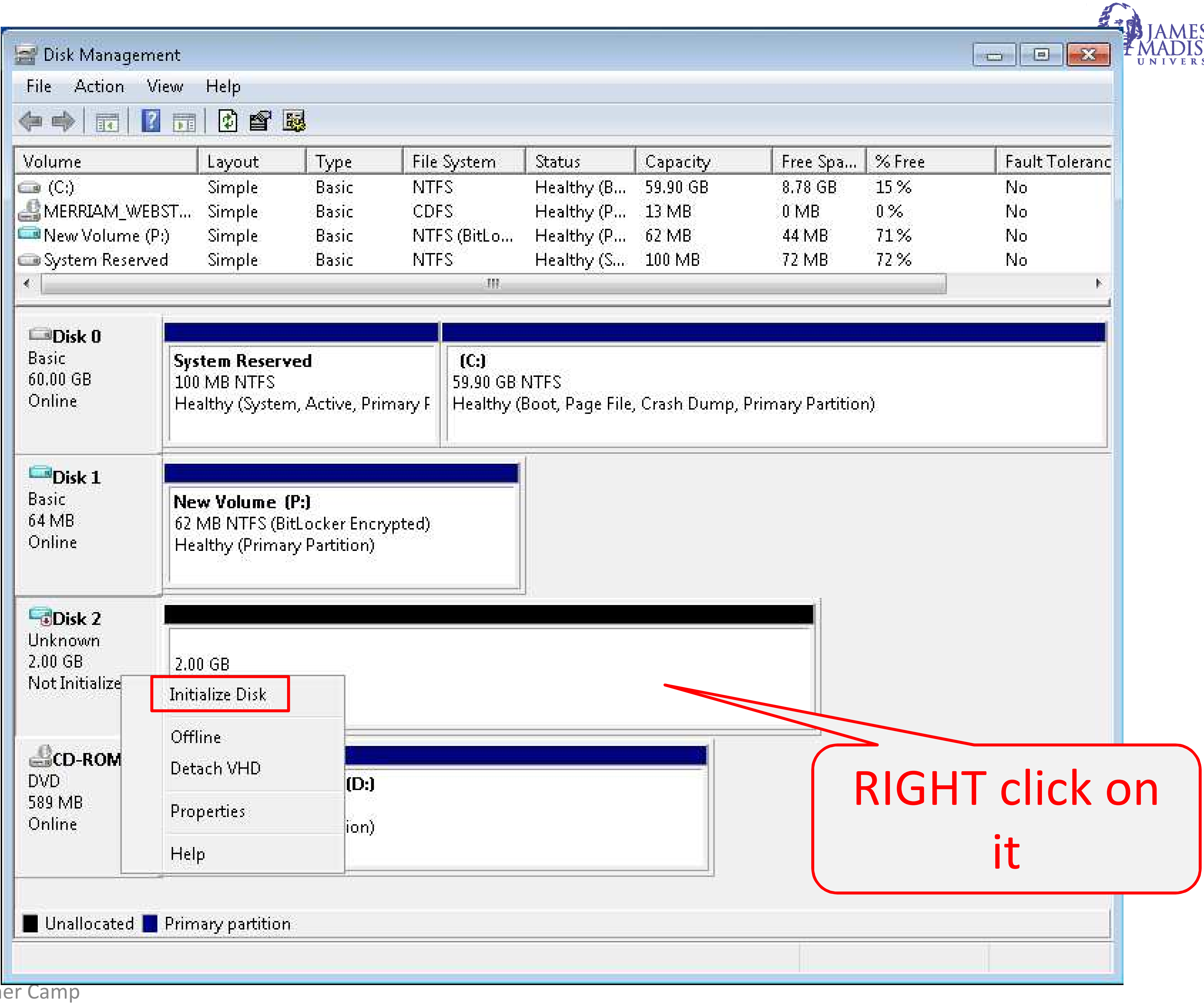
2.00 GB
Unallocated

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

This is the newly created drive



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	72 MB	72 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Unknown
2.00 GB
Not Initialize

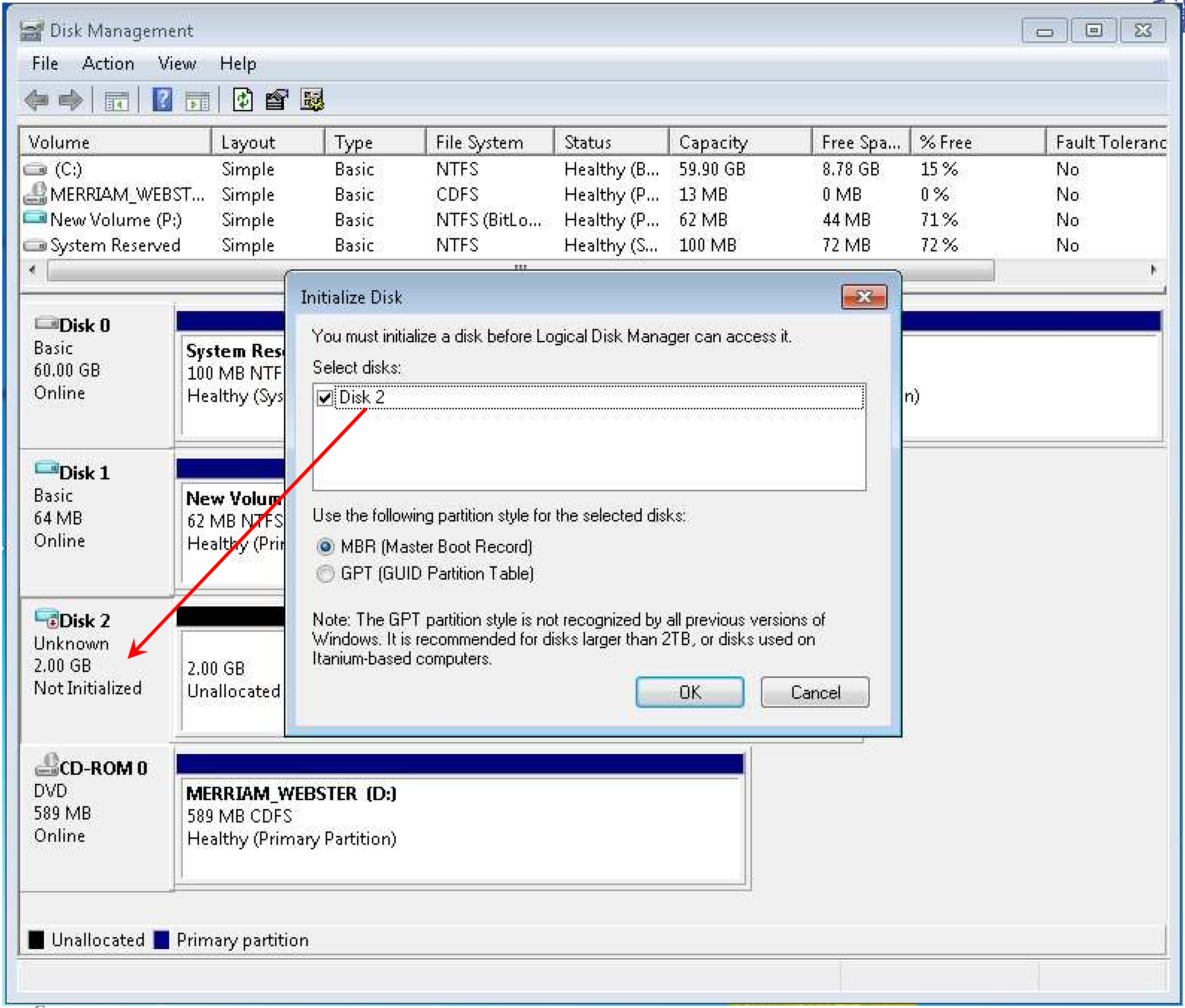
2.00 GB

CD-ROM
DVD
589 MB
Online

(D:)
ion)

■ Unallocated ■ Primary partition

RIGHT click on it



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	72 MB	72 %	No

Disk 0
Basic
60.00 GB
Online

System Res
100 MB NTF
Healthy (Sys

Disk 1
Basic
64 MB
Online

New Volum
62 MB NTFS
Healthy (Pri

Disk 2
Unknown
2.00 GB
Not Initialized

2.00 GB
Unallocated

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

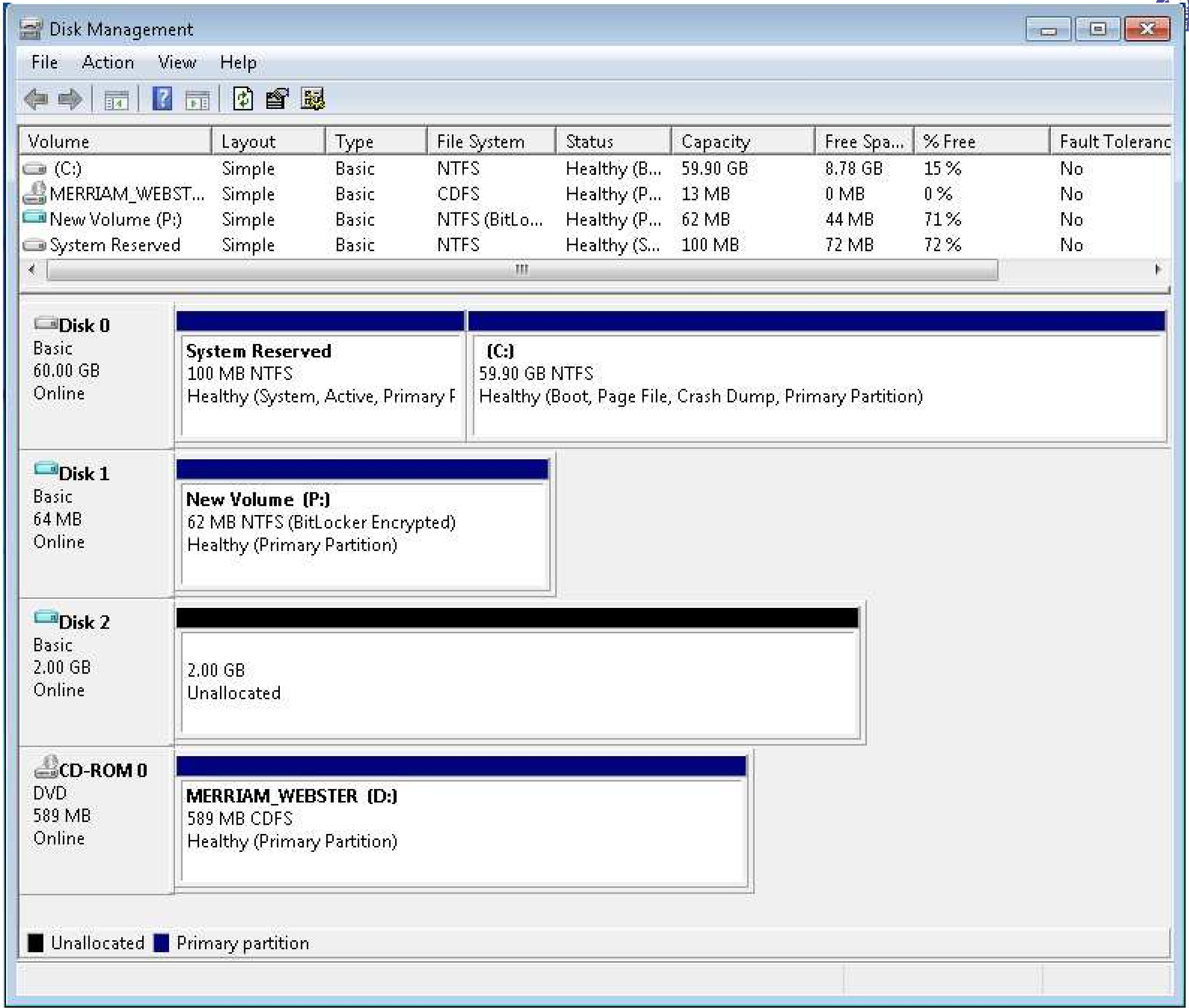
☑ Disk 2

Use the following partition style for the selected disks:

● MBR (Master Boot Record)

○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disks used on Itanium-based computers.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	72 MB	72 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

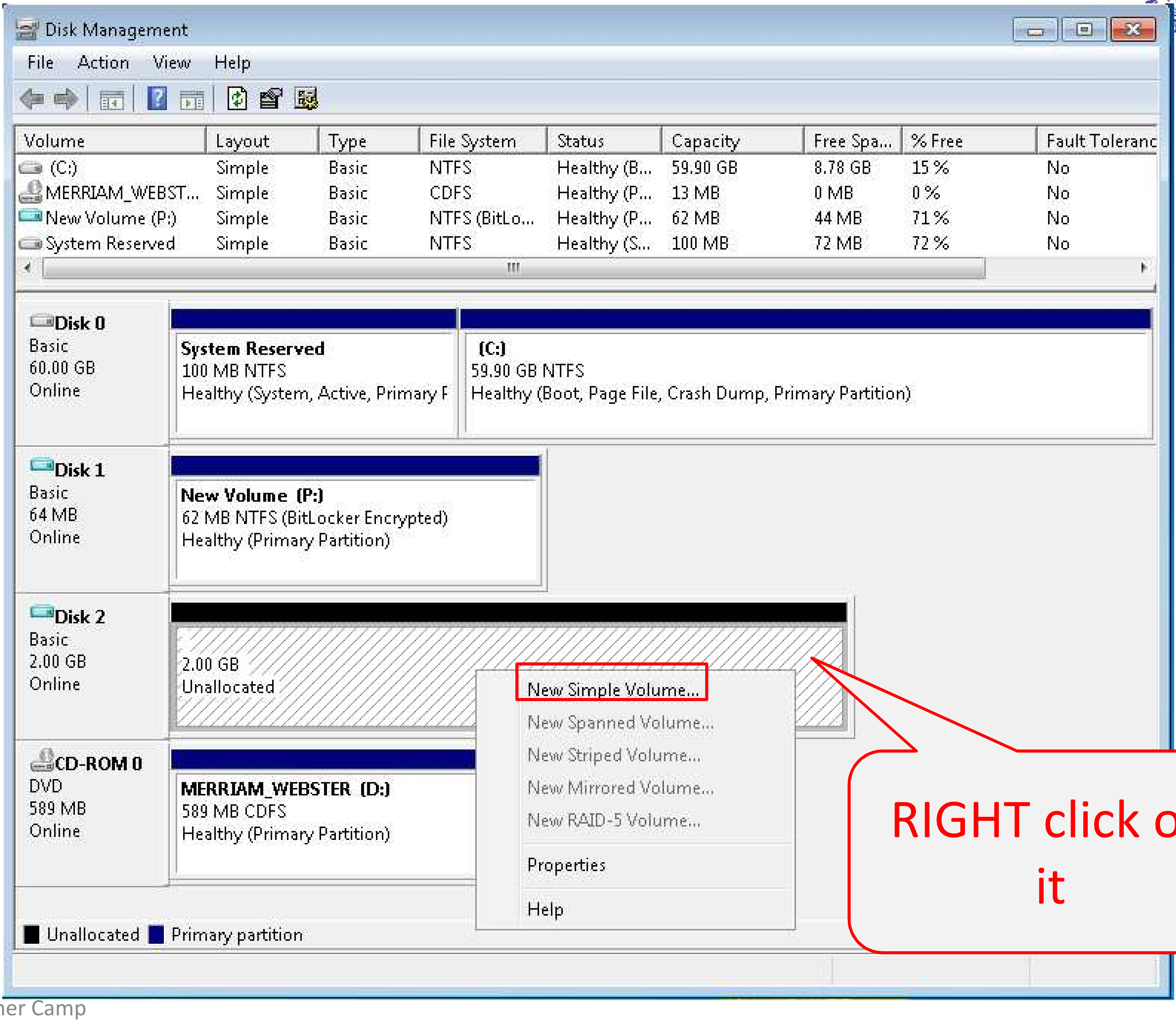
Disk 2
Basic
2.00 GB
Online

2.00 GB
Unallocated

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated 🟦 Primary partition



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	72 MB	72 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

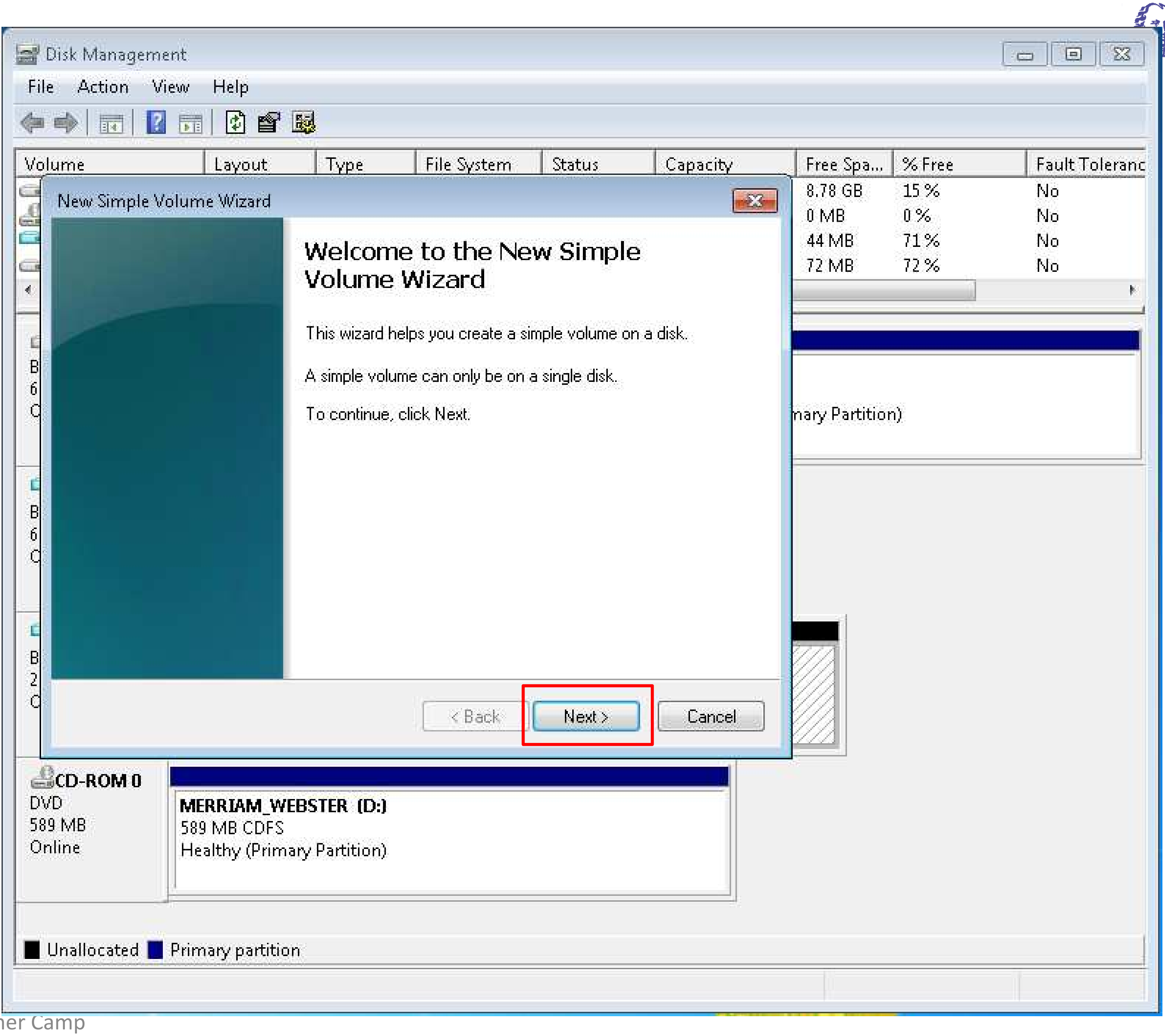
Disk 2
Basic
2.00 GB
Online

2.00 GB
Unallocated

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

RIGHT click on it



Free Spa...	% Free	Fault Toleranc
8.78 GB	15 %	No
0 MB	0 %	No
44 MB	71 %	No
72 MB	72 %	No

New Simple Volume Wizard

Welcome to the New Simple Volume Wizard

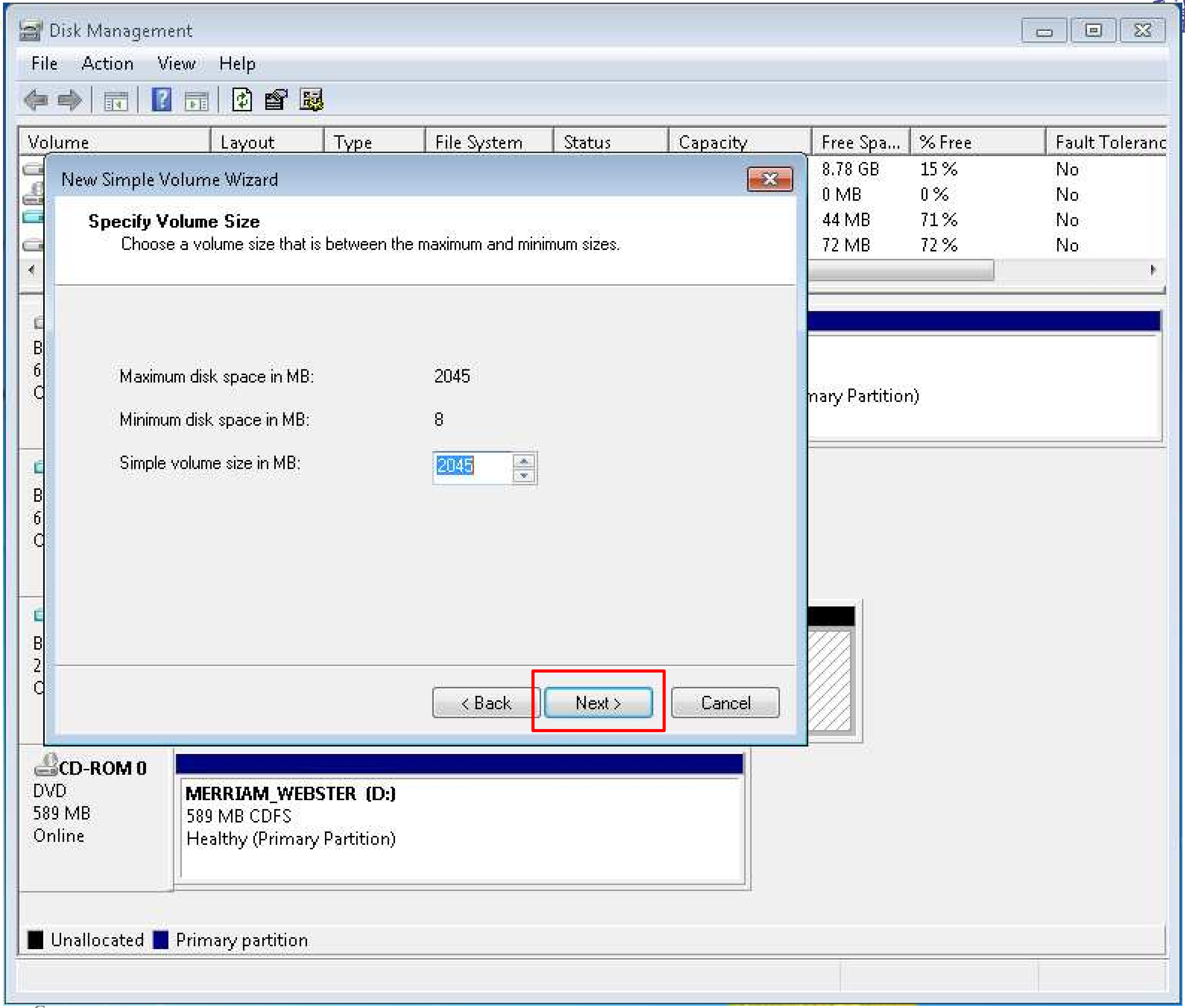
This wizard helps you create a simple volume on a disk.

A simple volume can only be on a single disk.

To continue, click Next.

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
						8.78 GB	15 %	No
						0 MB	0 %	No
						44 MB	71 %	No
						72 MB	72 %	No

New Simple Volume Wizard

Specify Volume Size

Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 2045

Minimum disk space in MB: 8

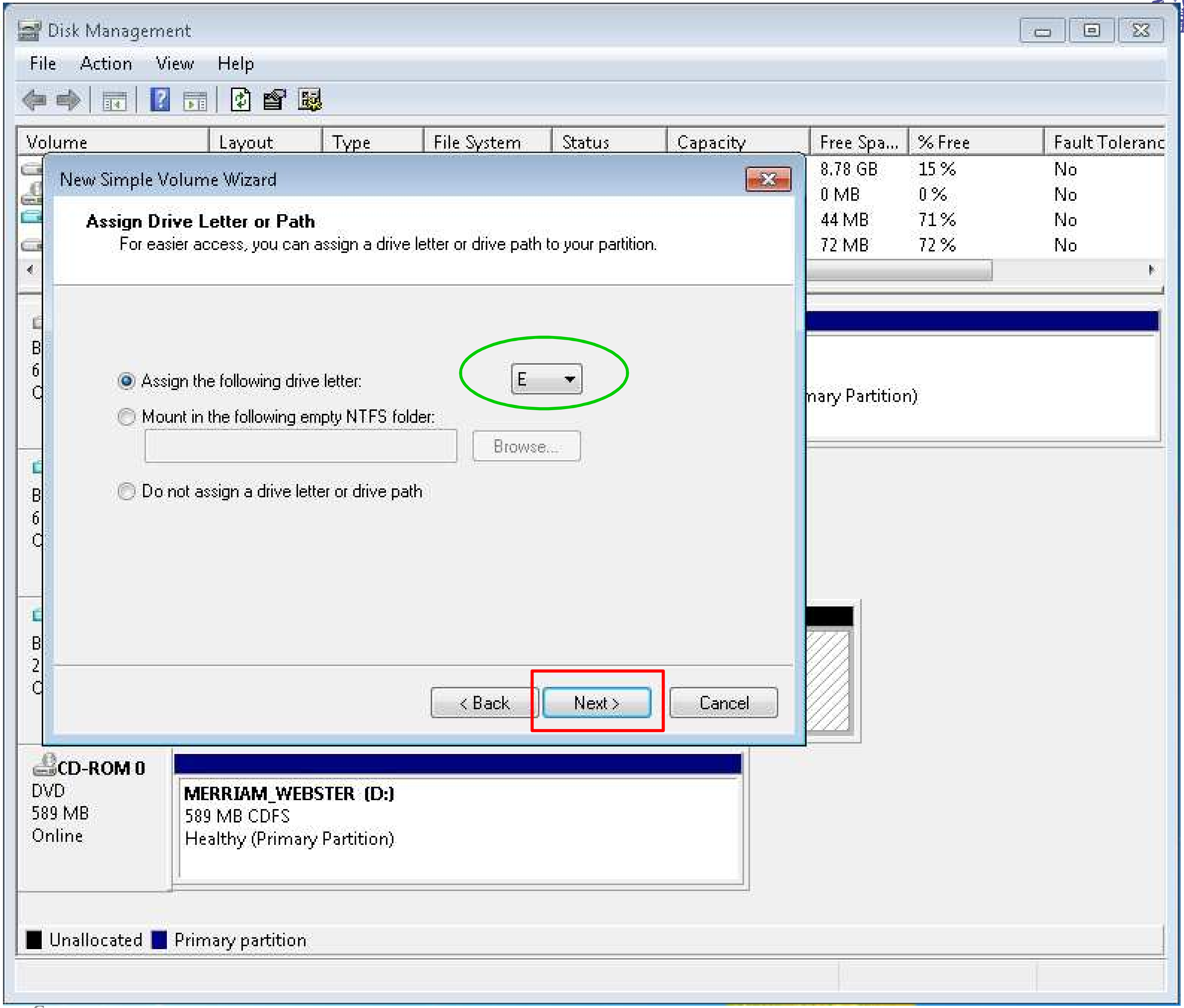
Simple volume size in MB: 2045

nary Partition)

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
						8.78 GB	15 %	No
						0 MB	0 %	No
						44 MB	71 %	No
						72 MB	72 %	No

New Simple Volume Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: E

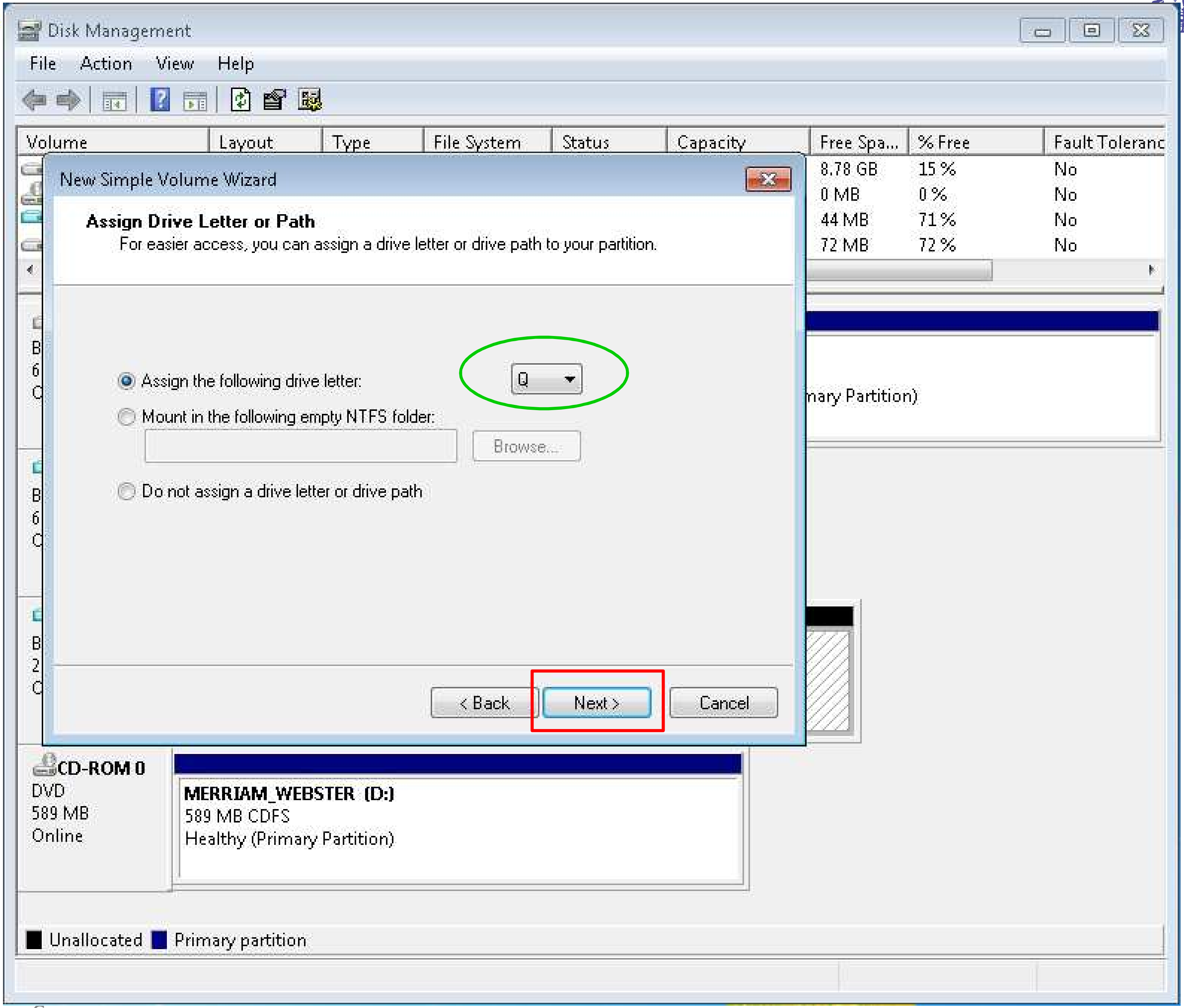
○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
						8.78 GB	15 %	No
						0 MB	0 %	No
						44 MB	71 %	No
						72 MB	72 %	No

New Simple Volume Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: Q

○ Mount in the following empty NTFS folder:

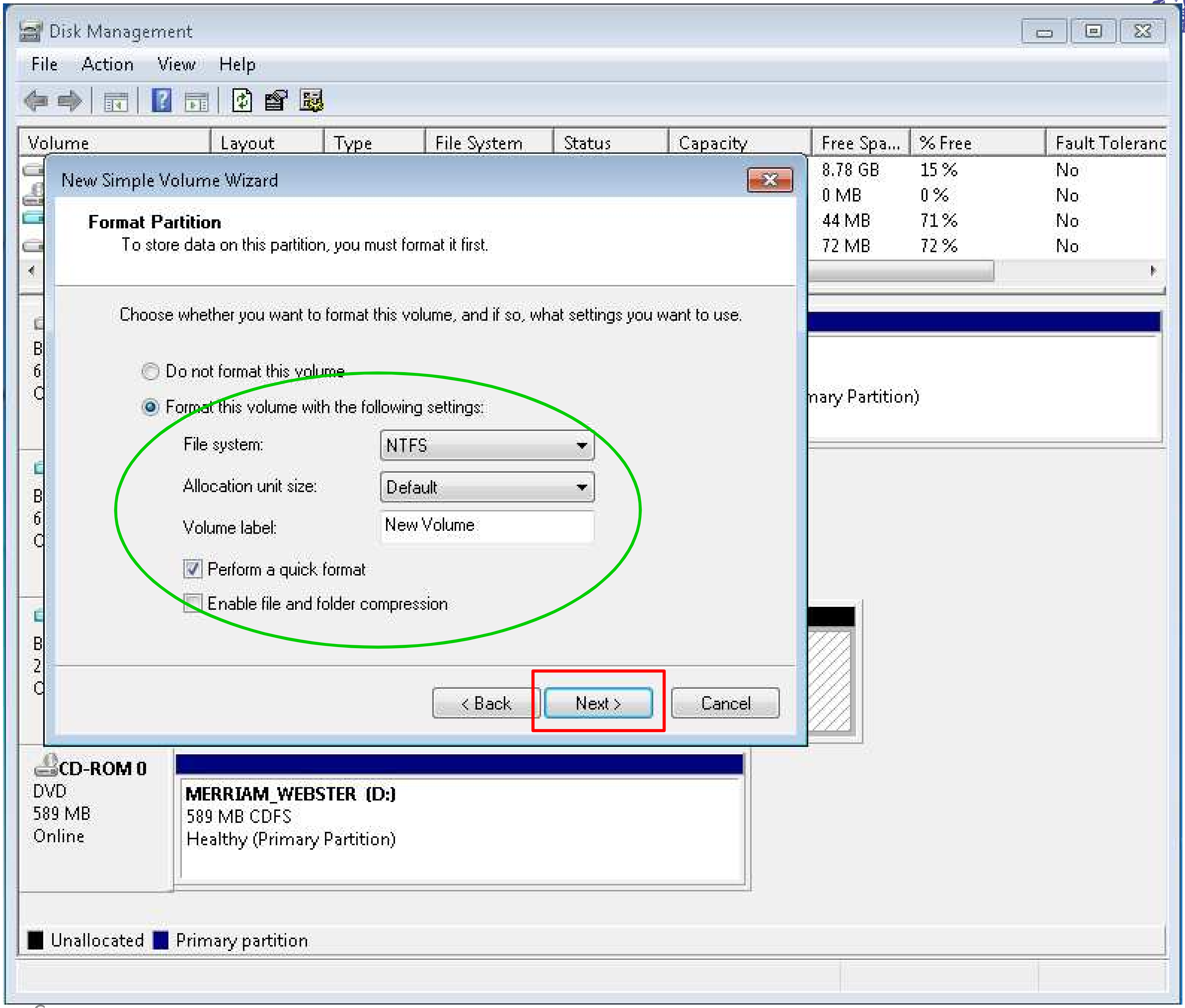
○ Do not assign a drive letter or drive path

nary Partition)

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



Free Spa...	% Free	Fault Toleranc
8.78 GB	15 %	No
0 MB	0 %	No
44 MB	71 %	No
72 MB	72 %	No

New Simple Volume Wizard

Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: New Volume

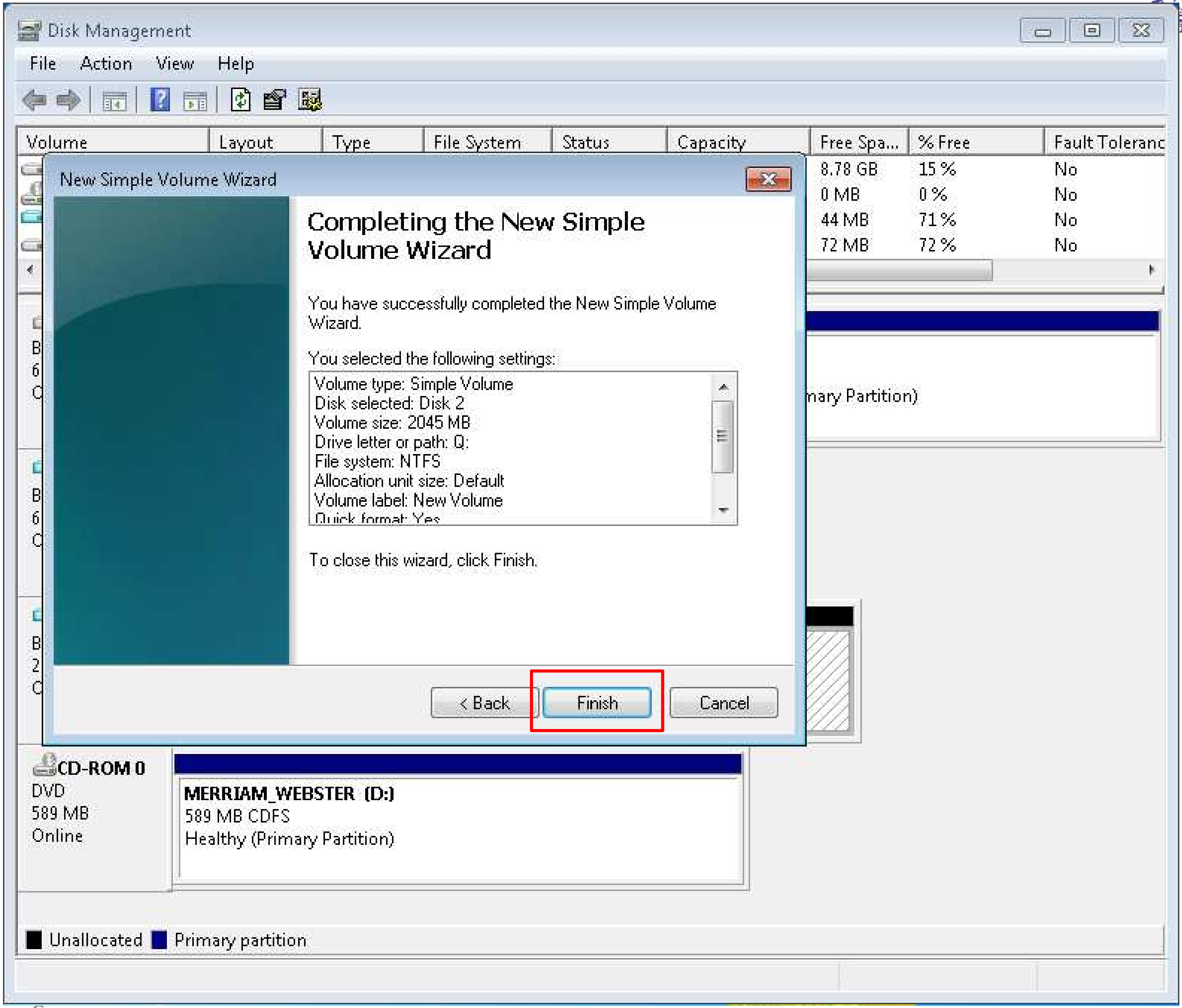
☑ Perform a quick format

□ Enable file and folder compression

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition



New Simple Volume Wizard

Completing the New Simple Volume Wizard

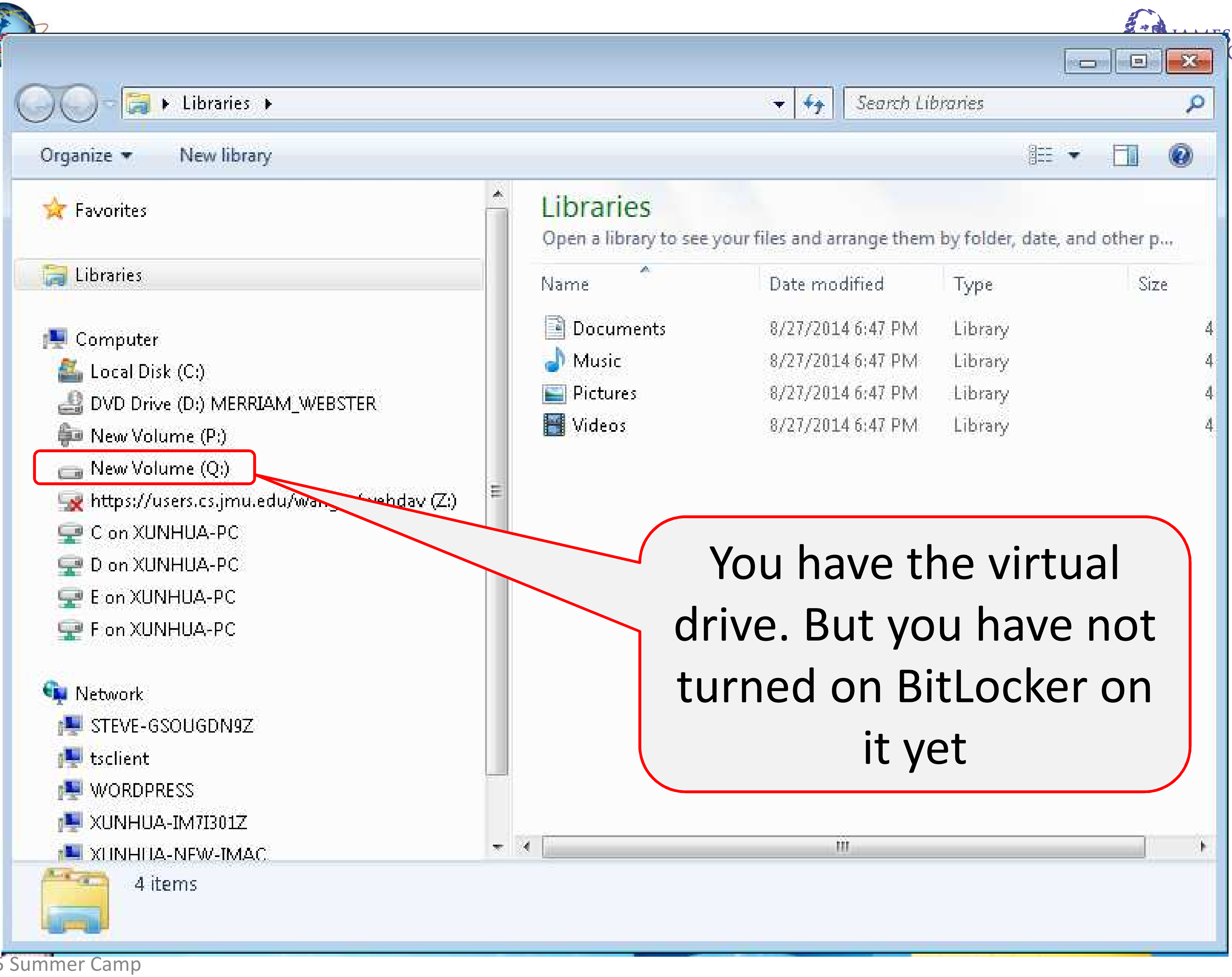
You have successfully completed the New Simple Volume Wizard.

You selected the following settings:

Volume type: Simple Volume
Disk selected: Disk 2
Volume size: 2045 MB
Drive letter or path: Q:
File system: NTFS
Allocation unit size: Default
Volume label: New Volume
Quick format: Yes

To close this wizard, click Finish.

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

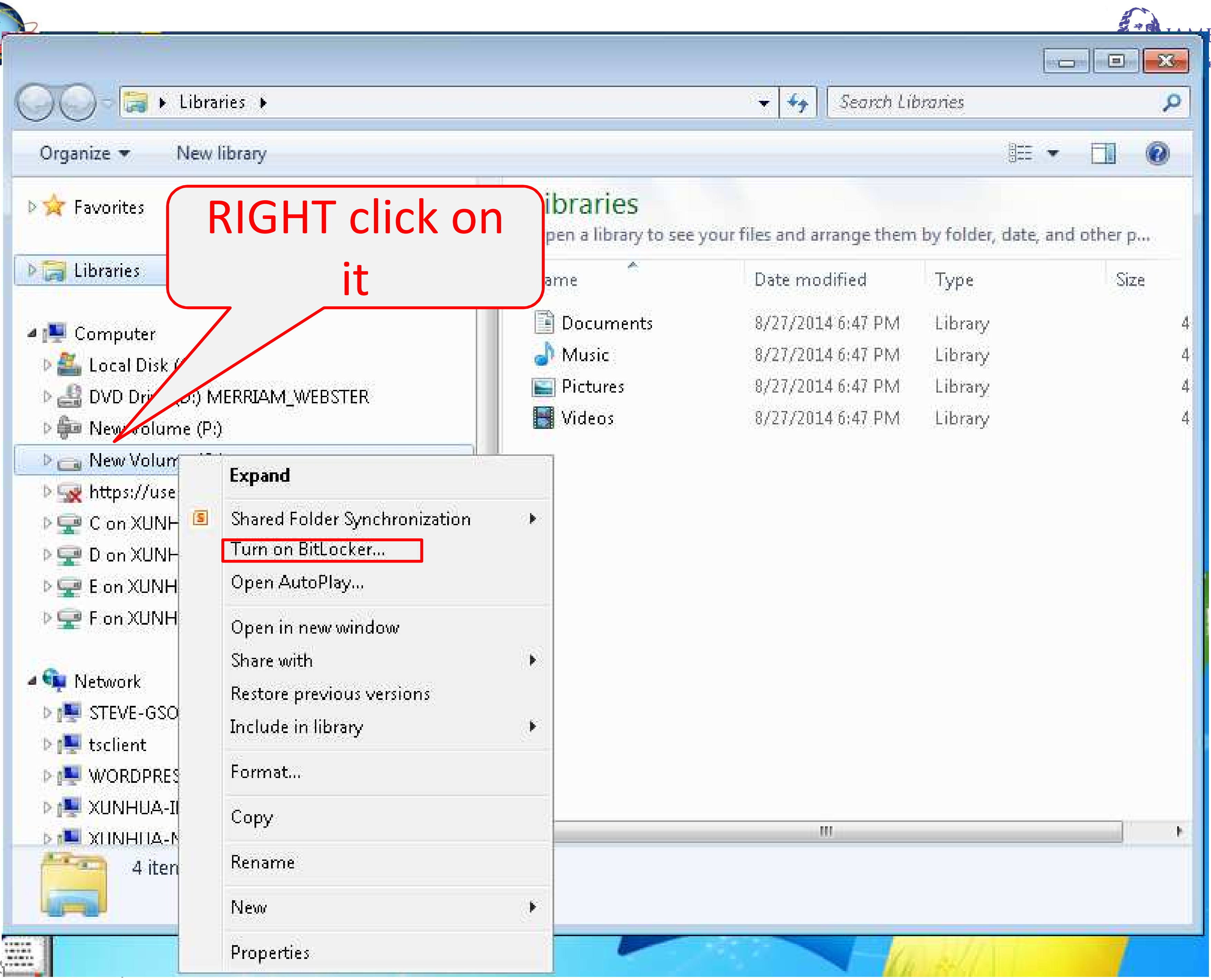


Libraries

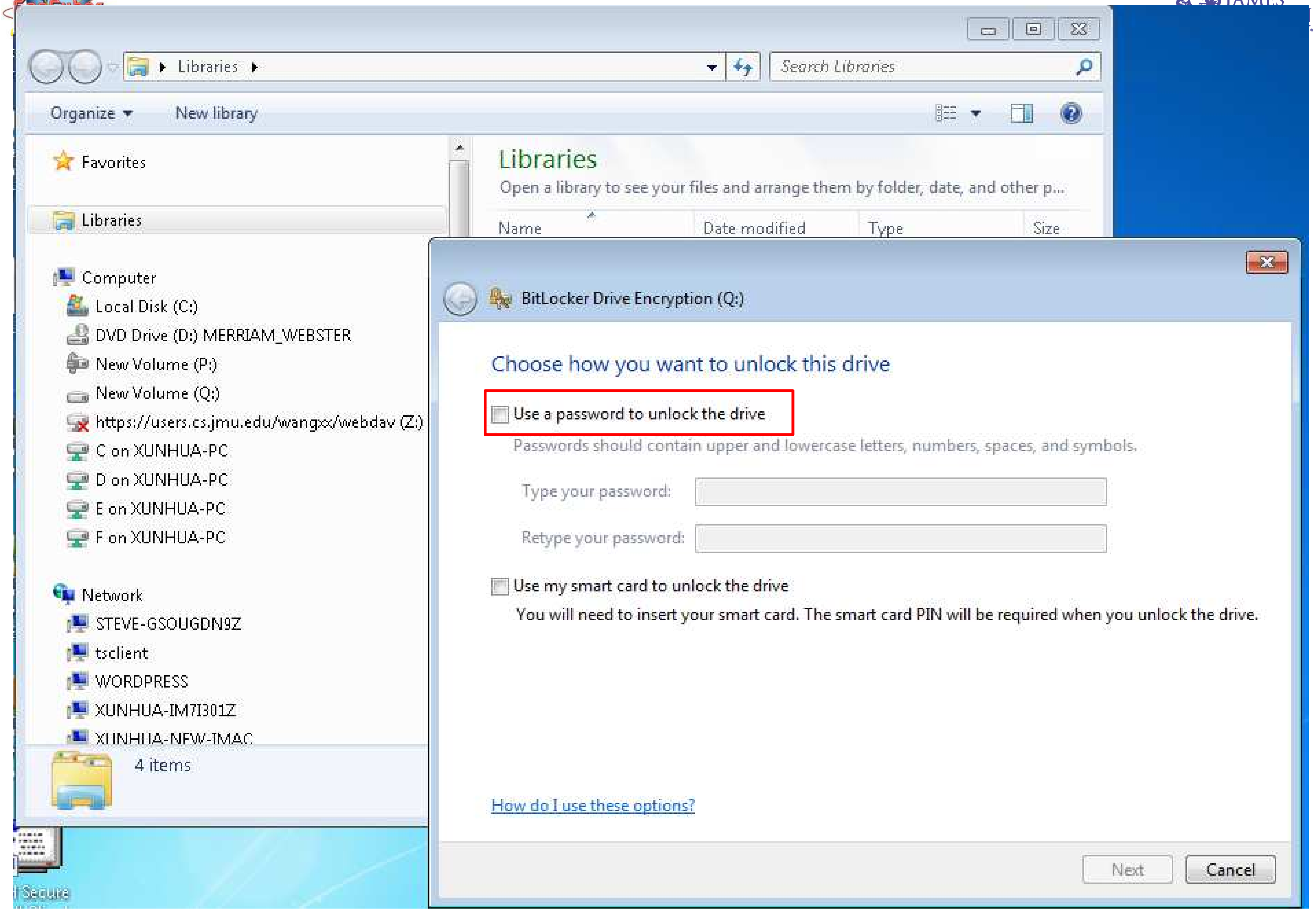
Open a library to see your files and arrange them by folder, date, and other p...

Name	Date modified	Type	Size
Documents	8/27/2014 6:47 PM	Library	4
Music	8/27/2014 6:47 PM	Library	4
Pictures	8/27/2014 6:47 PM	Library	4
Videos	8/27/2014 6:47 PM	Library	4

You have the virtual drive. But you have not turned on BitLocker on it yet



RIGHT click on it



BitLocker Drive Encryption (Q:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

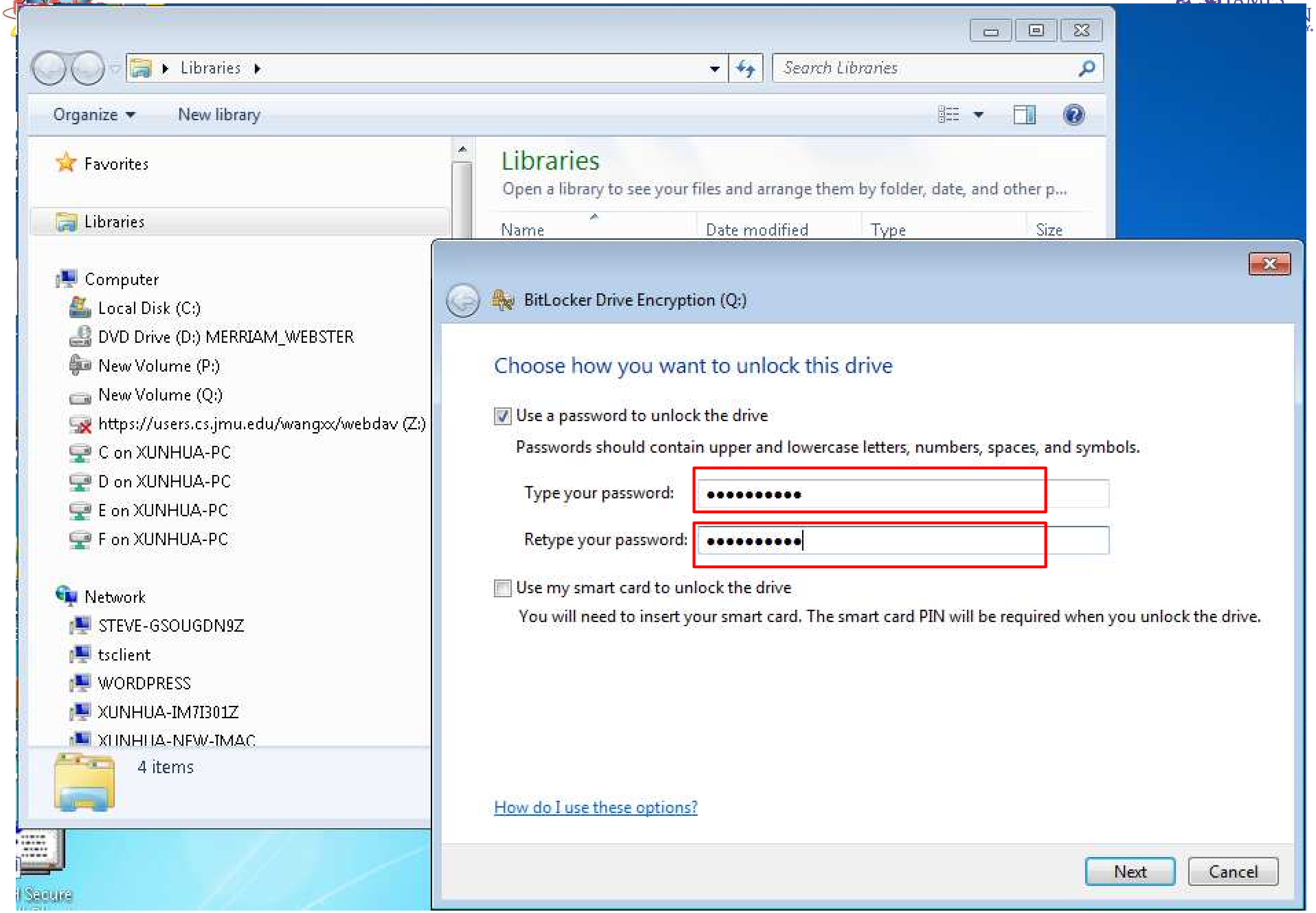
Type your password:

Retype your password:

□ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?



BitLocker Drive Encryption (Q:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

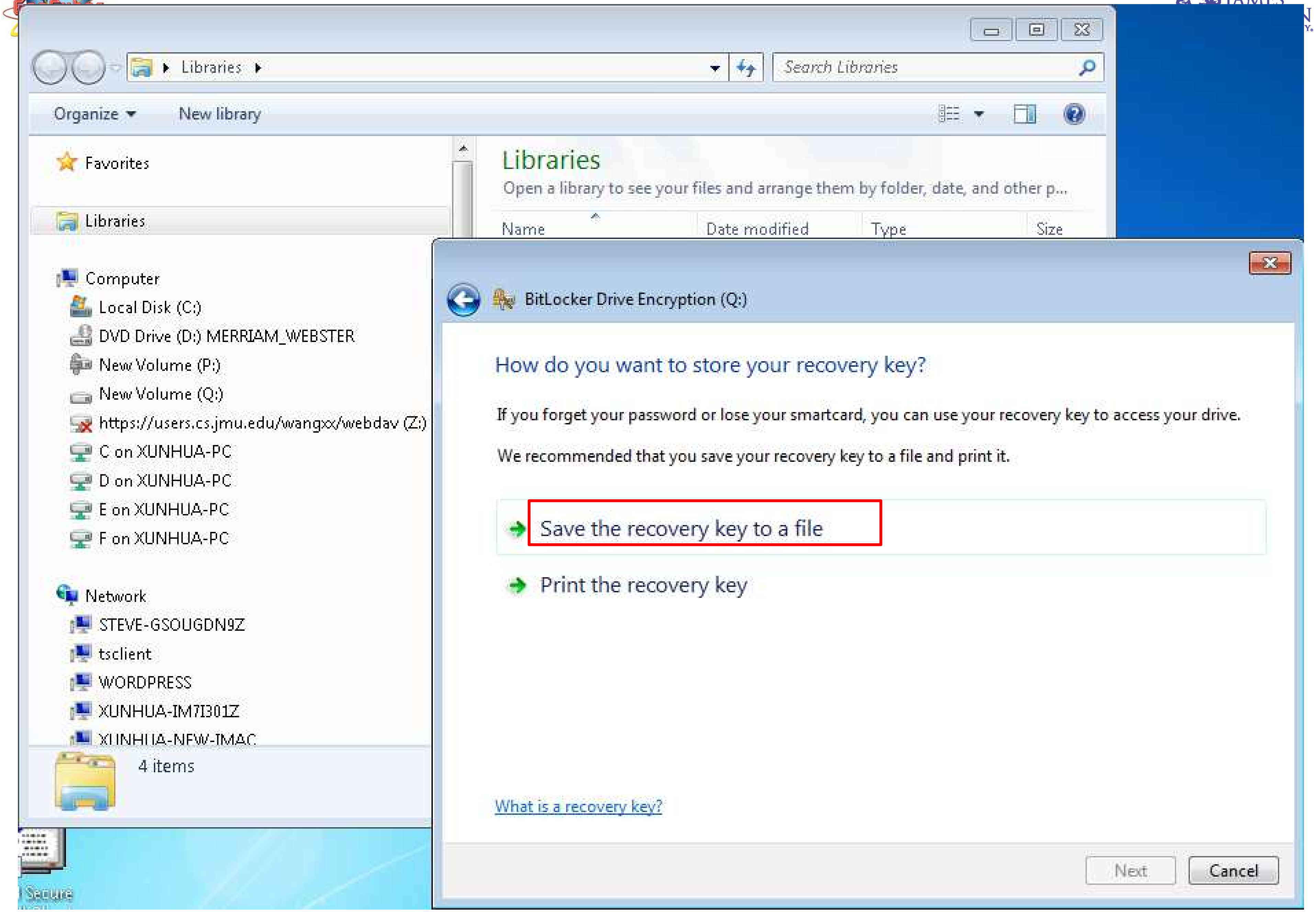
Type your password: ●●●●●●●●●●

Retype your password: ●●●●●●●●●●

☐ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?



BitLocker Drive Encryption (Q:)

How do you want to store your recovery key?

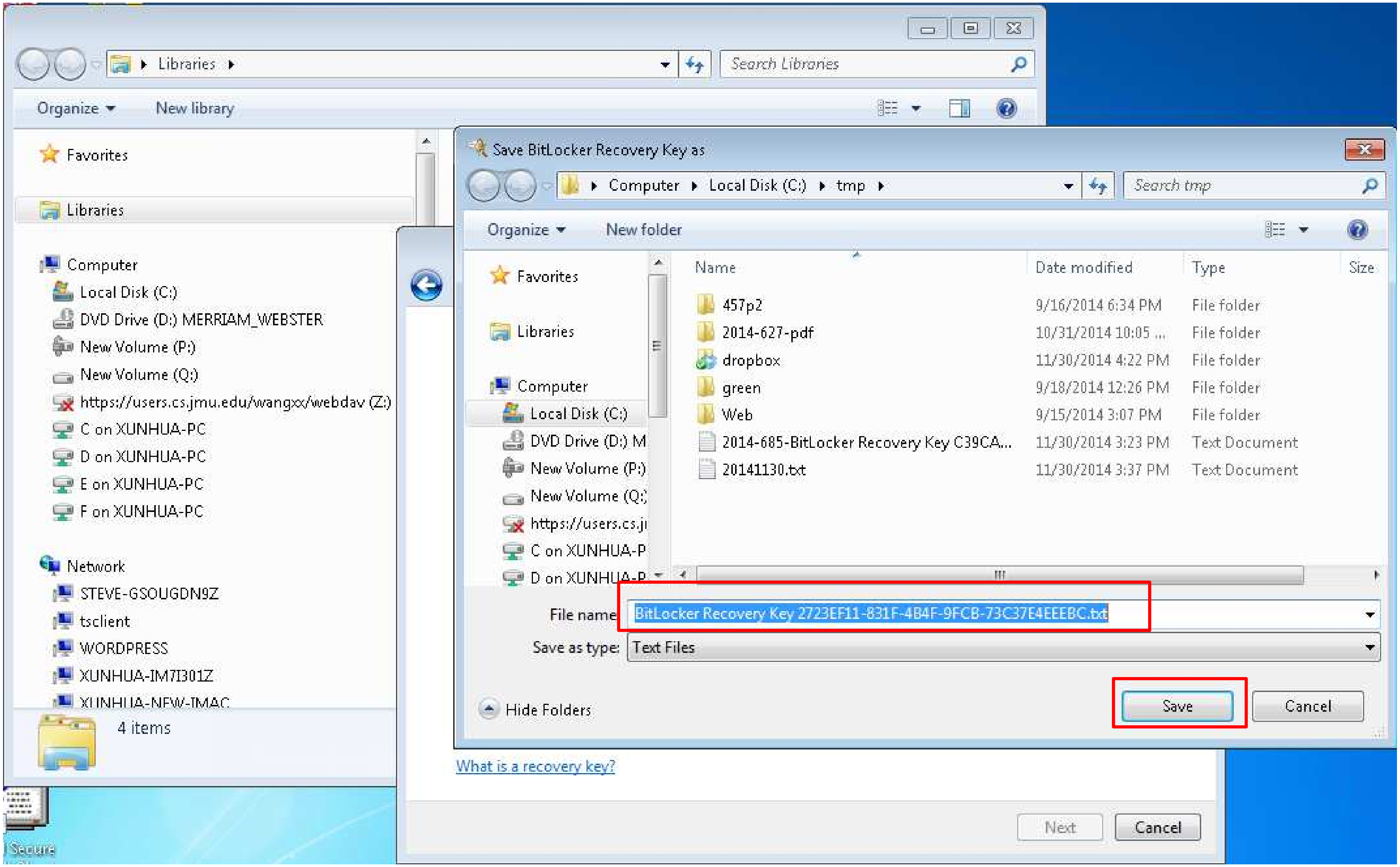
If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

We recommended that you save your recovery key to a file and print it.

→ Save the recovery key to a file

→ Print the recovery key

What is a recovery key?



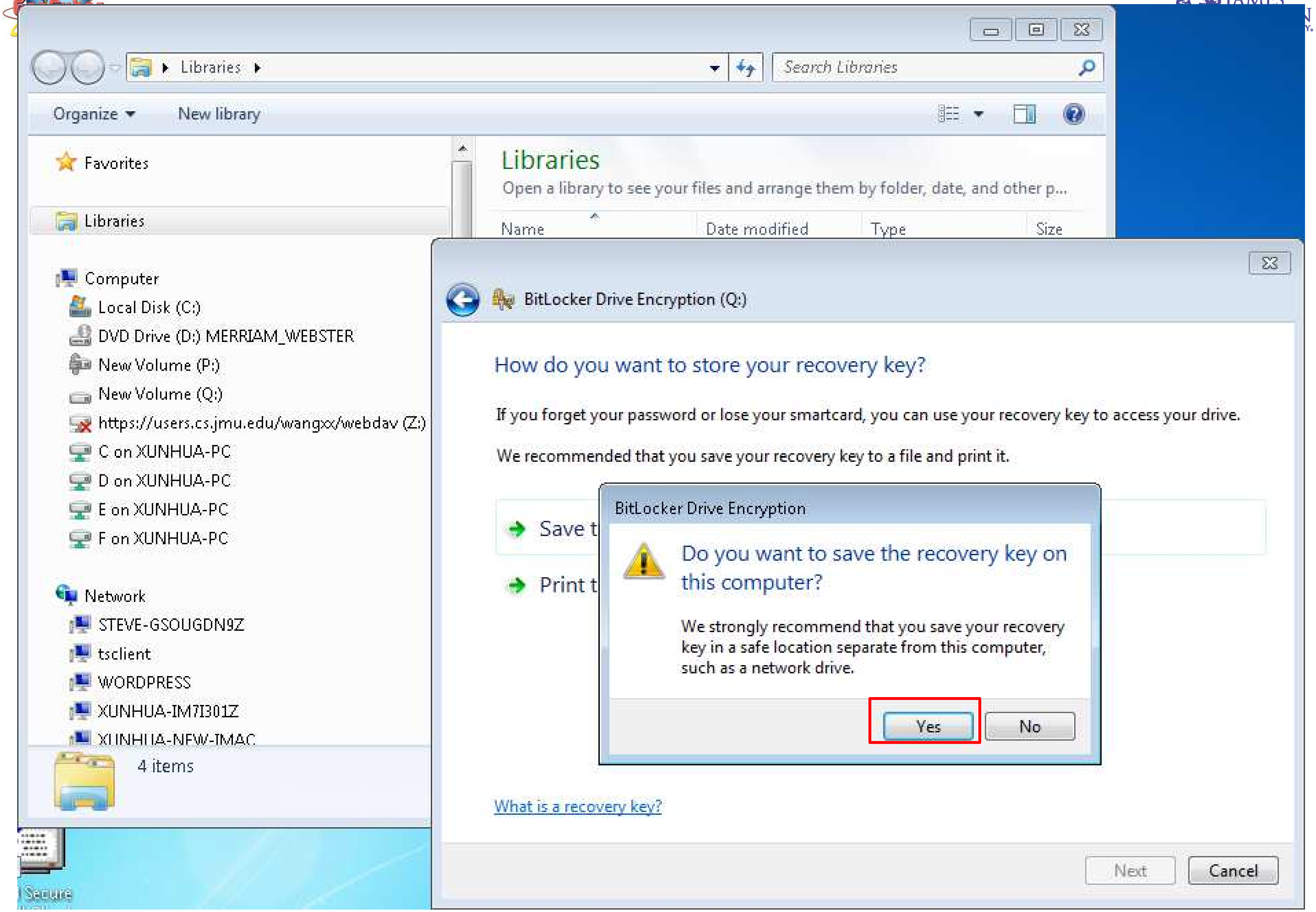
Save BitLocker Recovery Key as

Computer ▸ Local Disk (C:) ▸ tmp ▸

Name	Date modified	Type	Size
457p2	9/16/2014 6:34 PM	File folder	
2014-627-pdf	10/31/2014 10:05 ...	File folder	
dropbox	11/30/2014 4:22 PM	File folder	
green	9/18/2014 12:26 PM	File folder	
Web	9/15/2014 3:07 PM	File folder	
2014-685-BitLocker Recovery Key C39CA...	11/30/2014 3:23 PM	Text Document	
20141130.txt	11/30/2014 3:37 PM	Text Document	

File name: BitLocker Recovery Key 2723EF11-831F-4B4F-9FCB-73C37E4EEEBC.txt

Save as type: Text Files



Libraries

Open a library to see your files and arrange them by folder, date, and other p...

BitLocker Drive Encryption (Q:)

How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

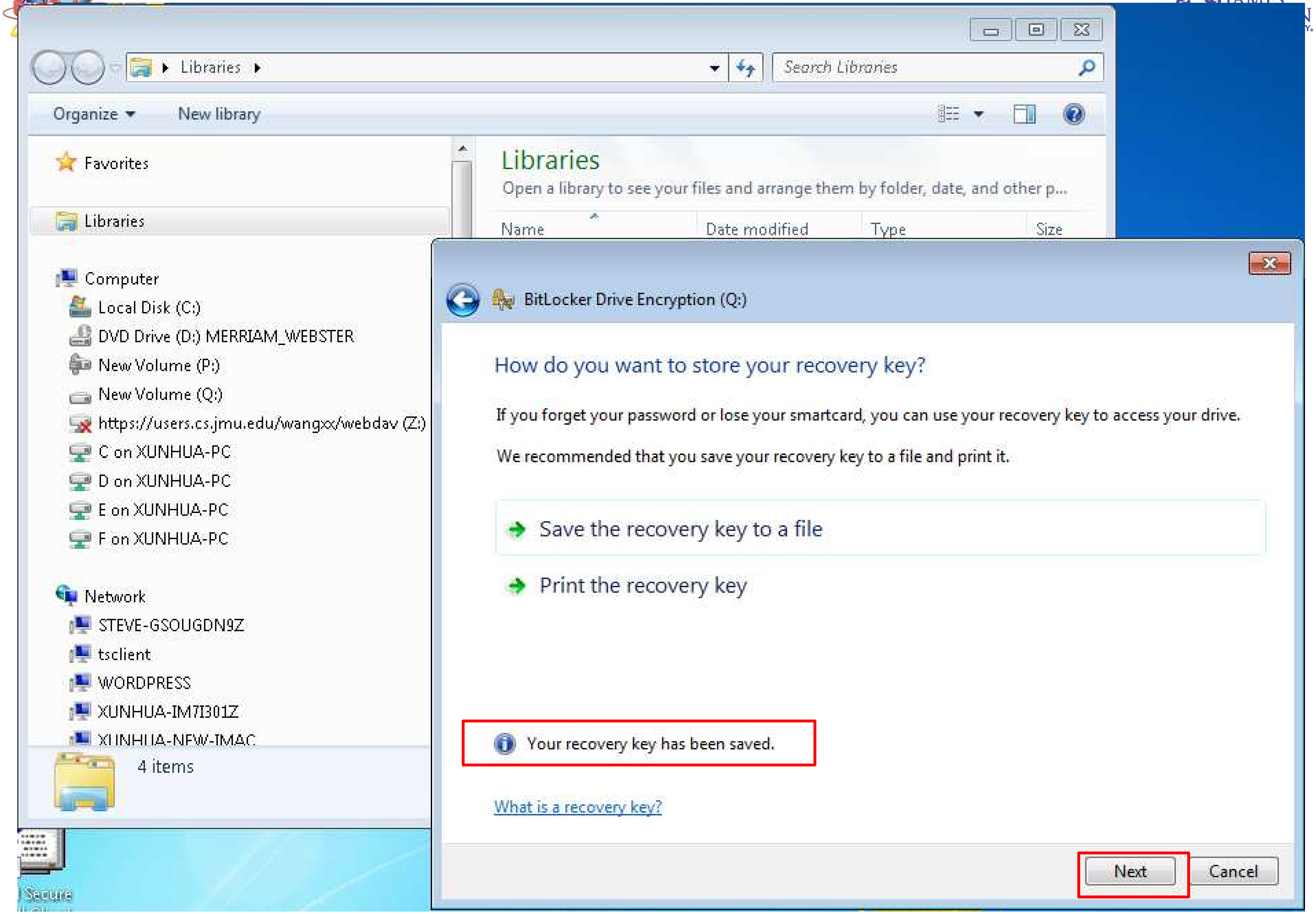
We recommended that you save your recovery key to a file and print it.

BitLocker Drive Encryption

Do you want to save the recovery key on this computer?

We strongly recommend that you save your recovery key in a safe location separate from this computer, such as a network drive.

What is a recovery key?



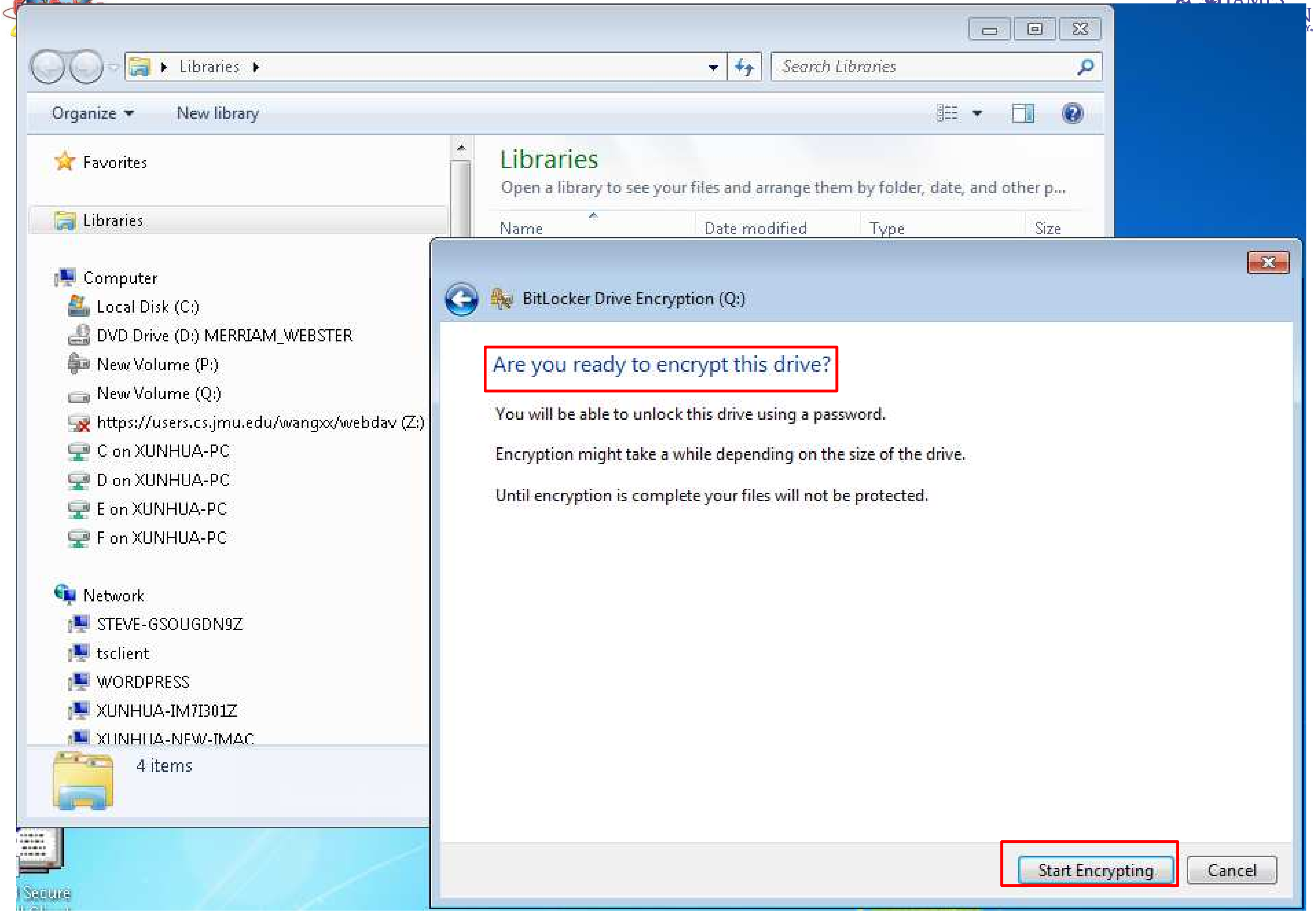
BitLocker Drive Encryption (Q:)

How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

We recommended that you save your recovery key to a file and print it.

Your recovery key has been saved.

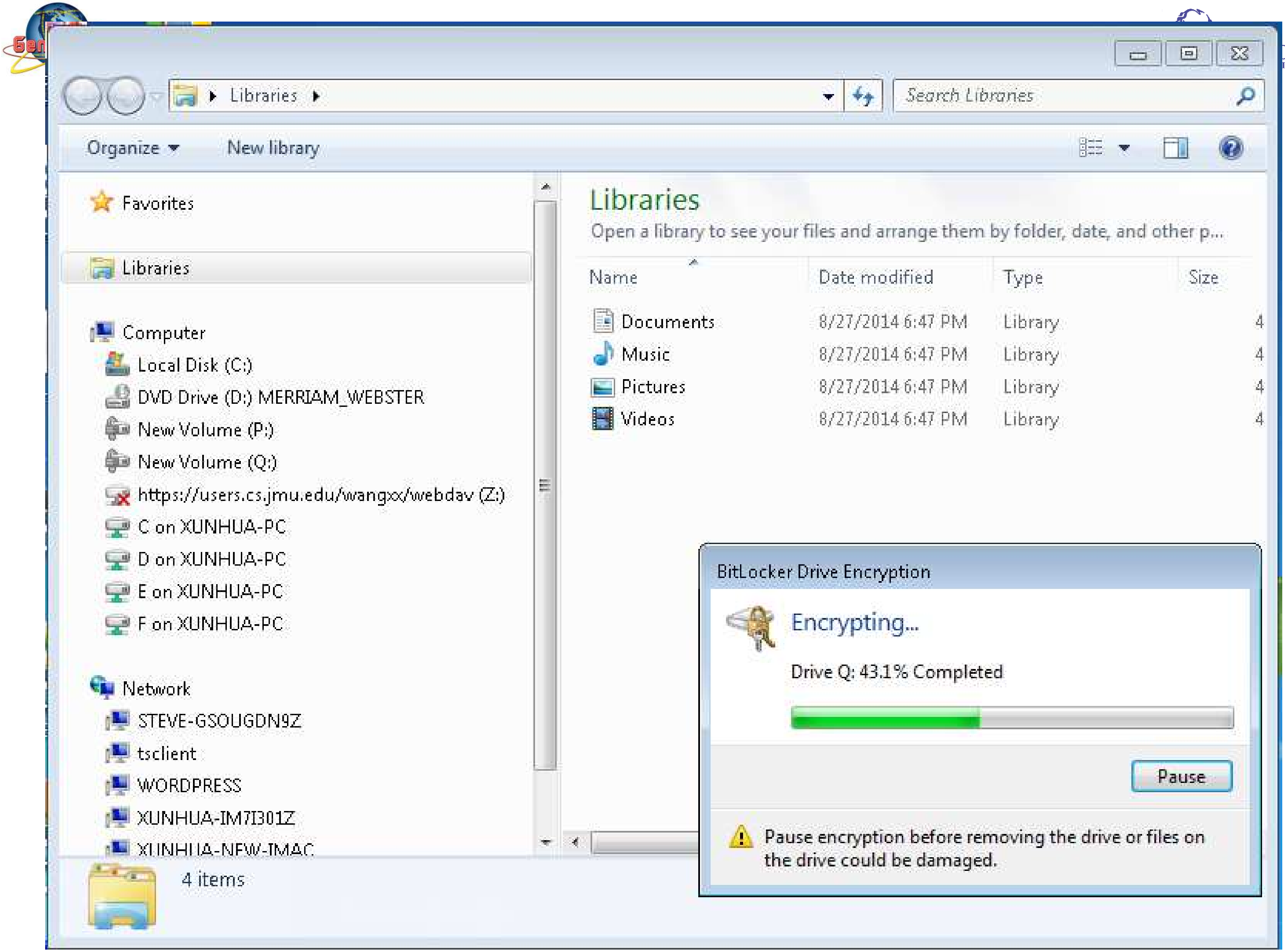


Are you ready to encrypt this drive?

You will be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete your files will not be protected.



Libraries

Open a library to see your files and arrange them by folder, date, and other p...

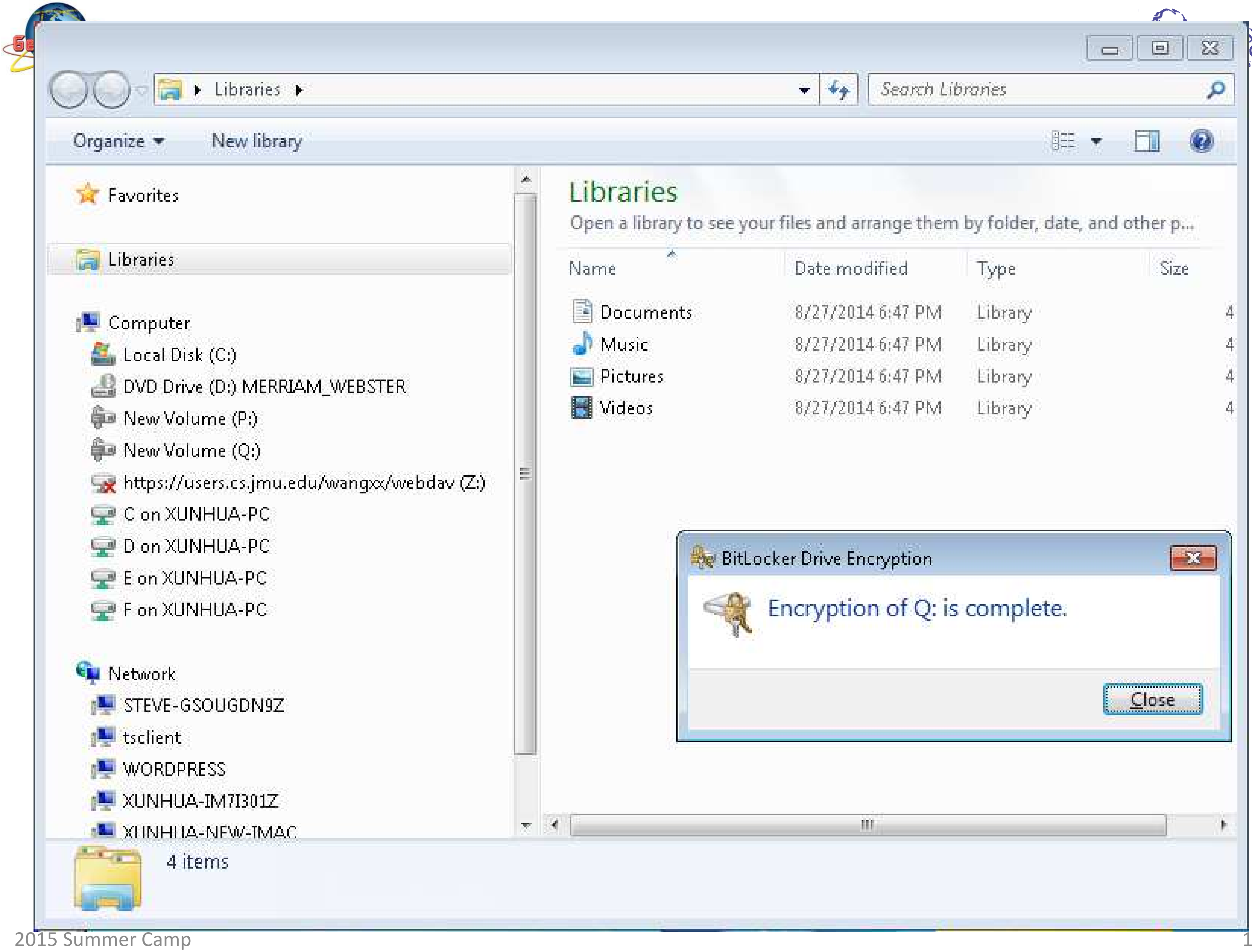
Name	Date modified	Type	Size
Documents	8/27/2014 6:47 PM	Library	4
Music	8/27/2014 6:47 PM	Library	4
Pictures	8/27/2014 6:47 PM	Library	4
Videos	8/27/2014 6:47 PM	Library	4

BitLocker Drive Encryption

Encrypting...

Drive Q: 43.1% Completed

⚠ Pause encryption before removing the drive or files on the drive could be damaged.



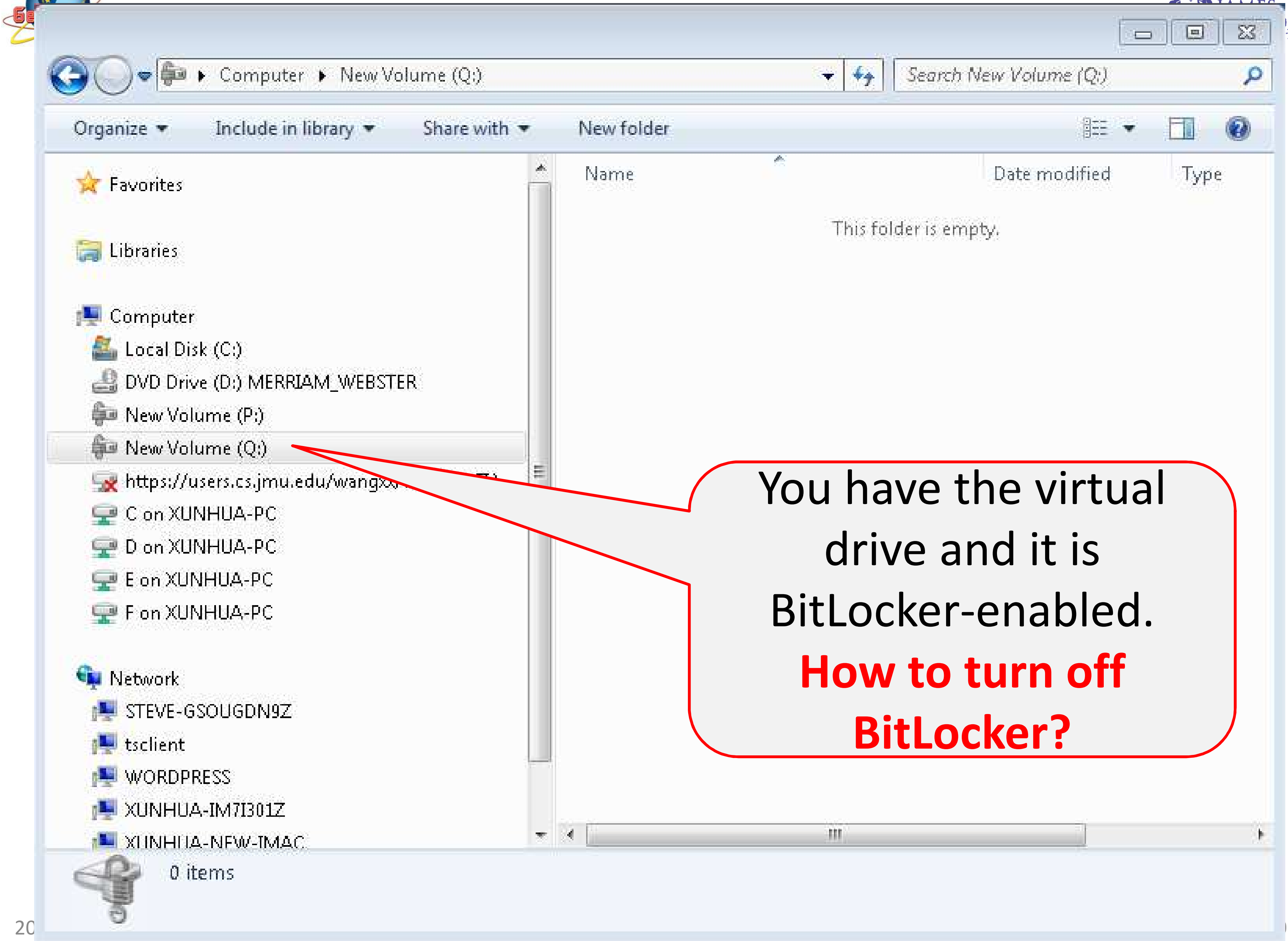
Libraries

Open a library to see your files and arrange them by folder, date, and other p...

Name	Date modified	Type	Size
Documents	8/27/2014 6:47 PM	Library	4
Music	8/27/2014 6:47 PM	Library	4
Pictures	8/27/2014 6:47 PM	Library	4
Videos	8/27/2014 6:47 PM	Library	4

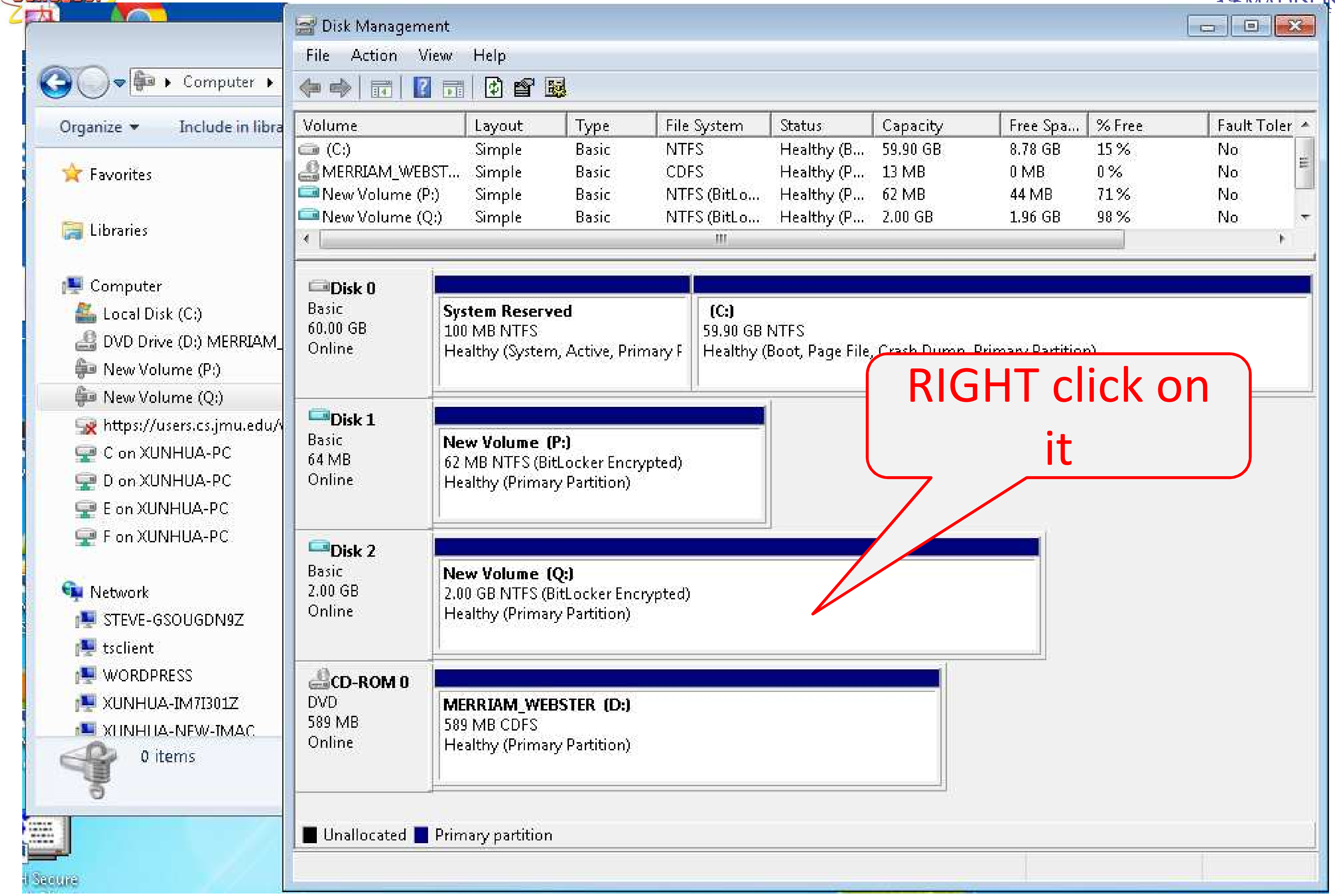
BitLocker Drive Encryption

Encryption of Q: is complete.



You have the virtual drive and it is BitLocker-enabled.

How to turn off BitLocker?



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toler
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
New Volume (Q:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	2.00 GB	1.96 GB	98 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Basic
2.00 GB
Online

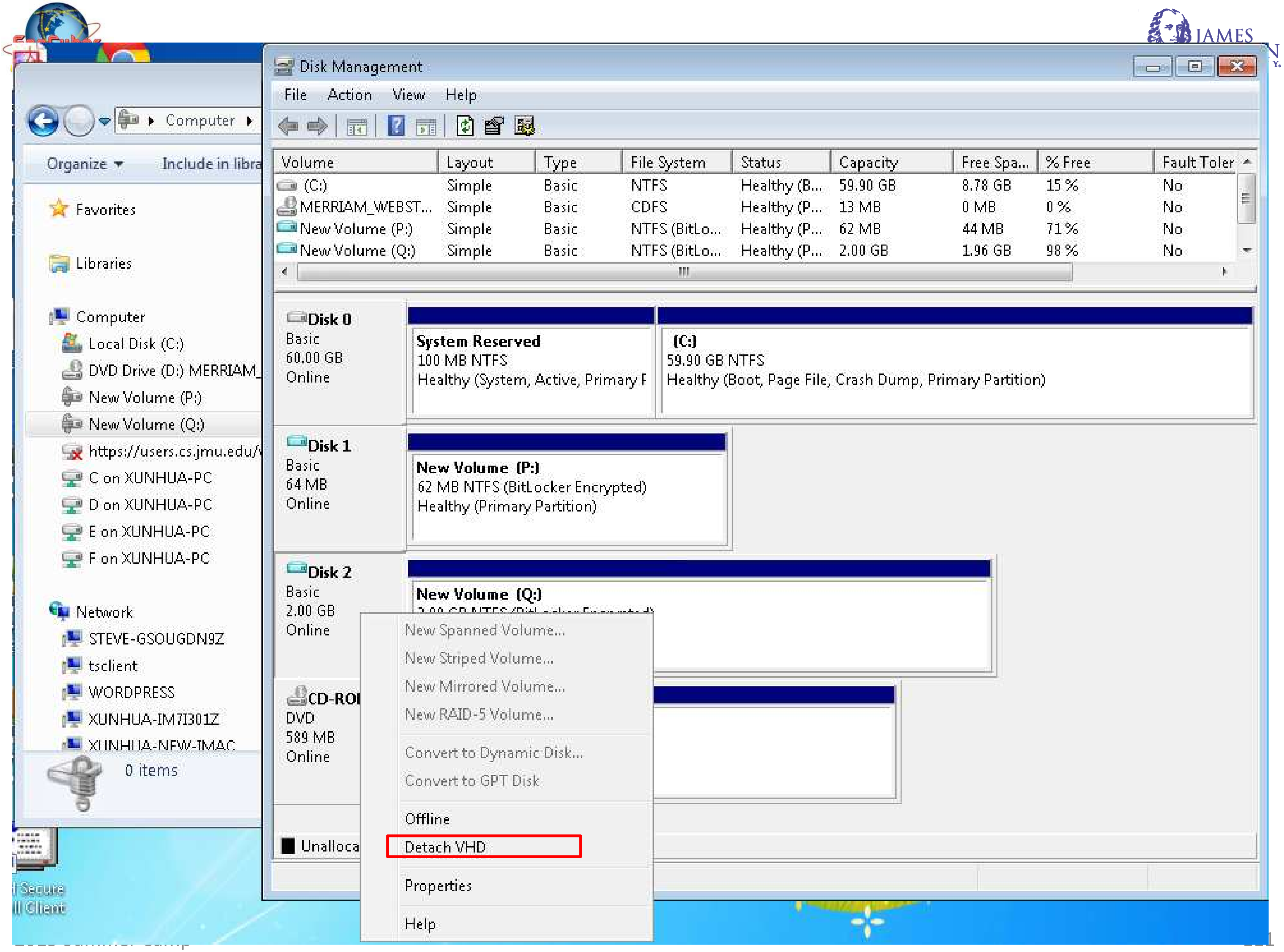
New Volume (Q:)
2.00 GB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

RIGHT click on it



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toler
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
New Volume (Q:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	2.00 GB	1.96 GB	98 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

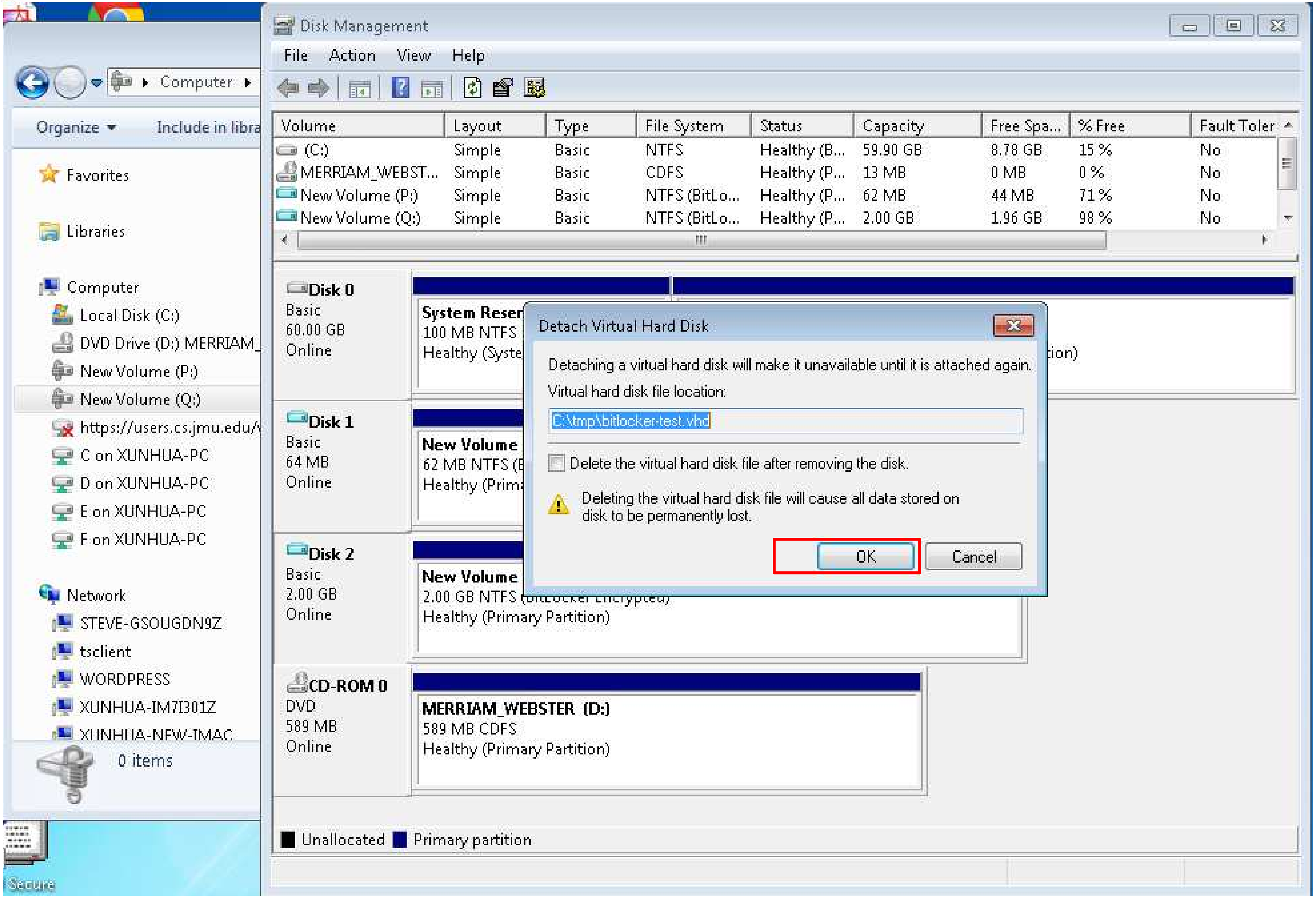
New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Basic
2.00 GB
Online

New Volume (Q:)

CD-ROM
DVD
589 MB
Online

Unalloca



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toler
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
New Volume (Q:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	2.00 GB	1.96 GB	98 %	No

Disk 0
Basic
60.00 GB
Online

System Reser
100 MB NTFS
Healthy (Syste

tion)

Disk 1
Basic
64 MB
Online

New Volume
62 MB NTFS (B
Healthy (Prima

Disk 2
Basic
2.00 GB
Online

New Volume
2.00 GB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

Detach Virtual Hard Disk

Detaching a virtual hard disk will make it unavailable until it is attached again.

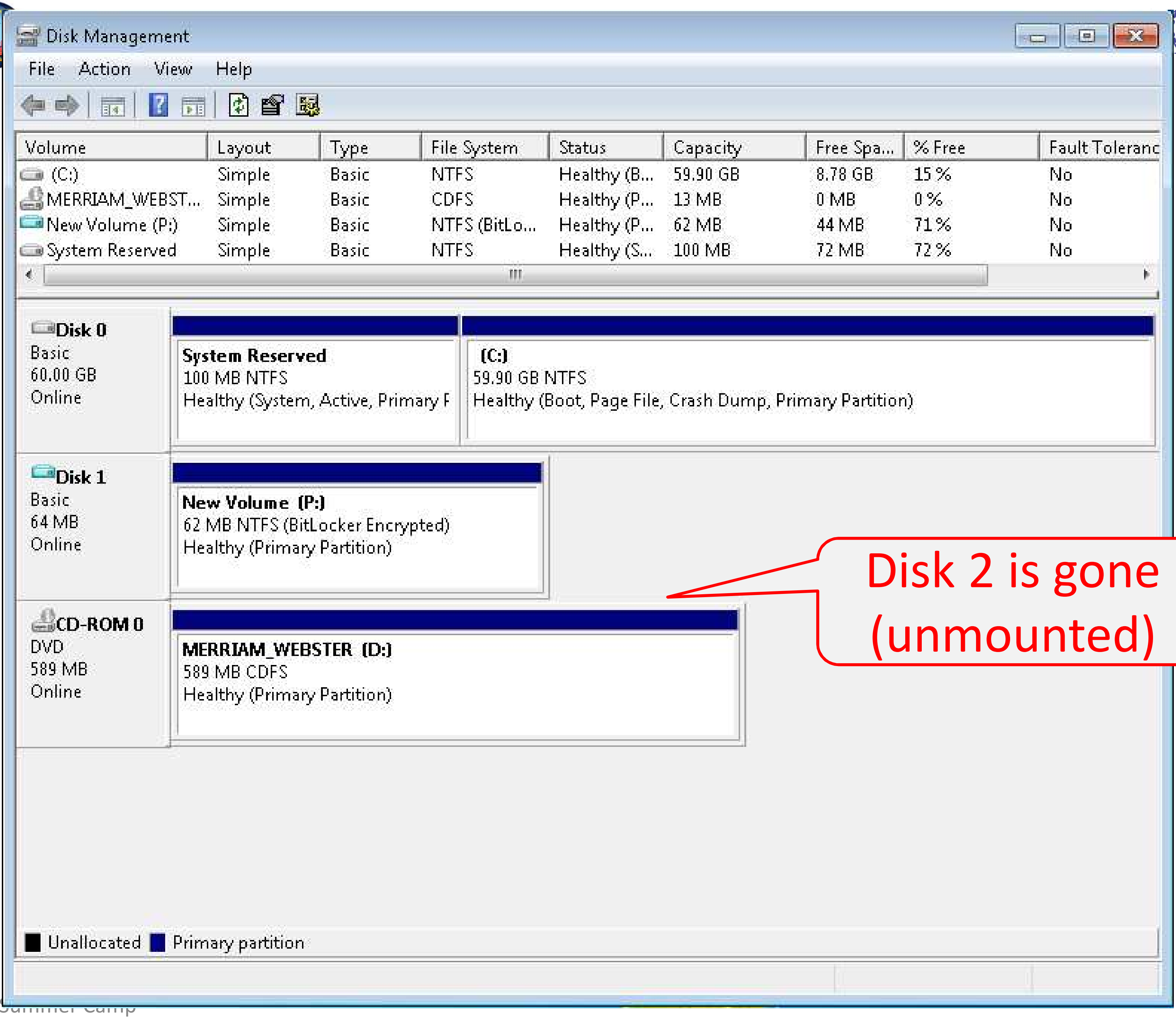
Virtual hard disk file location:

C:\tmp\bitlocker-test.vhd

□ Delete the virtual hard disk file after removing the disk.

⚠ Deleting the virtual hard disk file will cause all data stored on disk to be permanently lost.

OK Cancel



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toleranc
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
System Reserved	Simple	Basic	NTFS	Healthy (S...	100 MB	72 MB	72 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

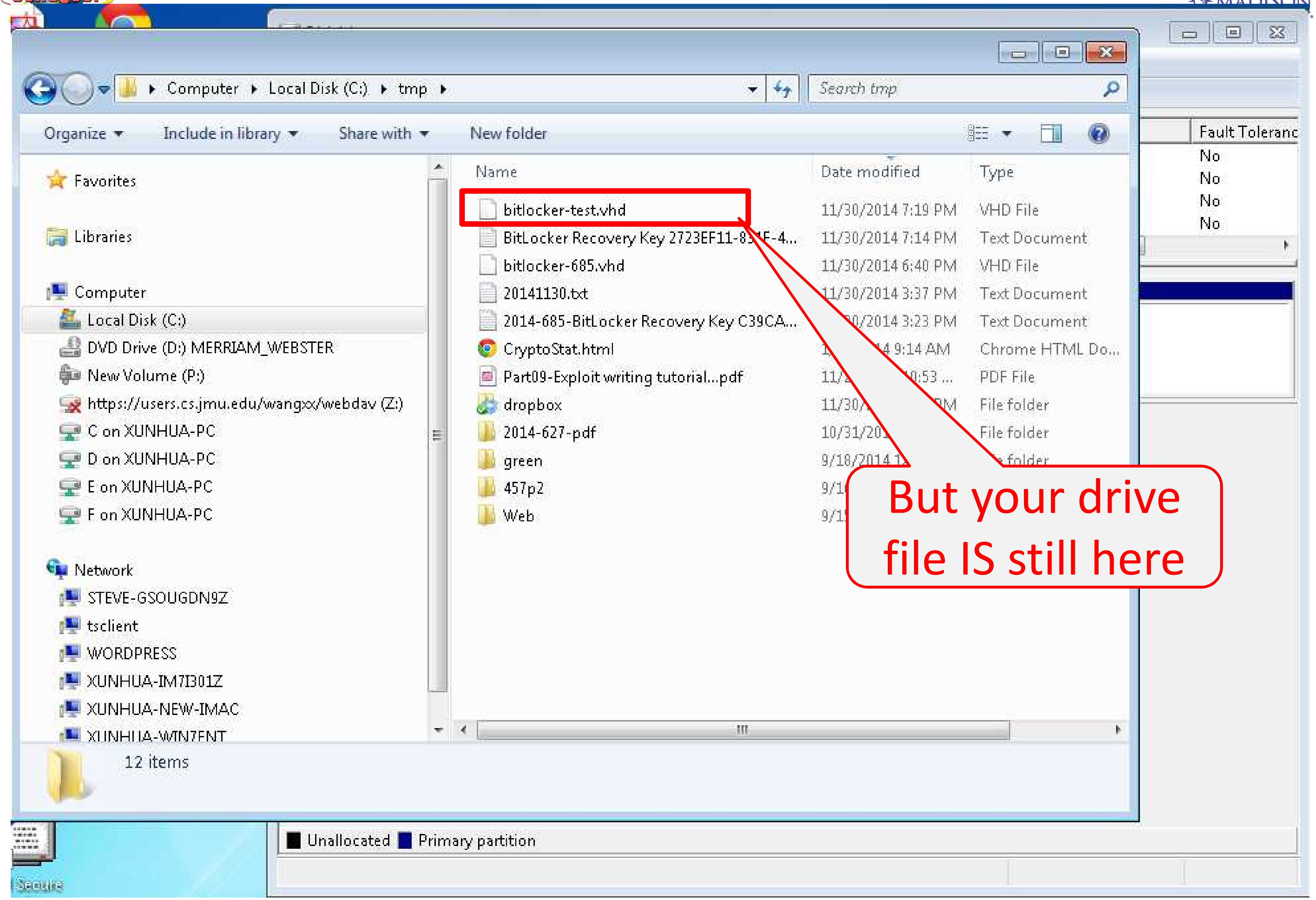
New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

CD-ROM 0
DVD
589 MB
Online

MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

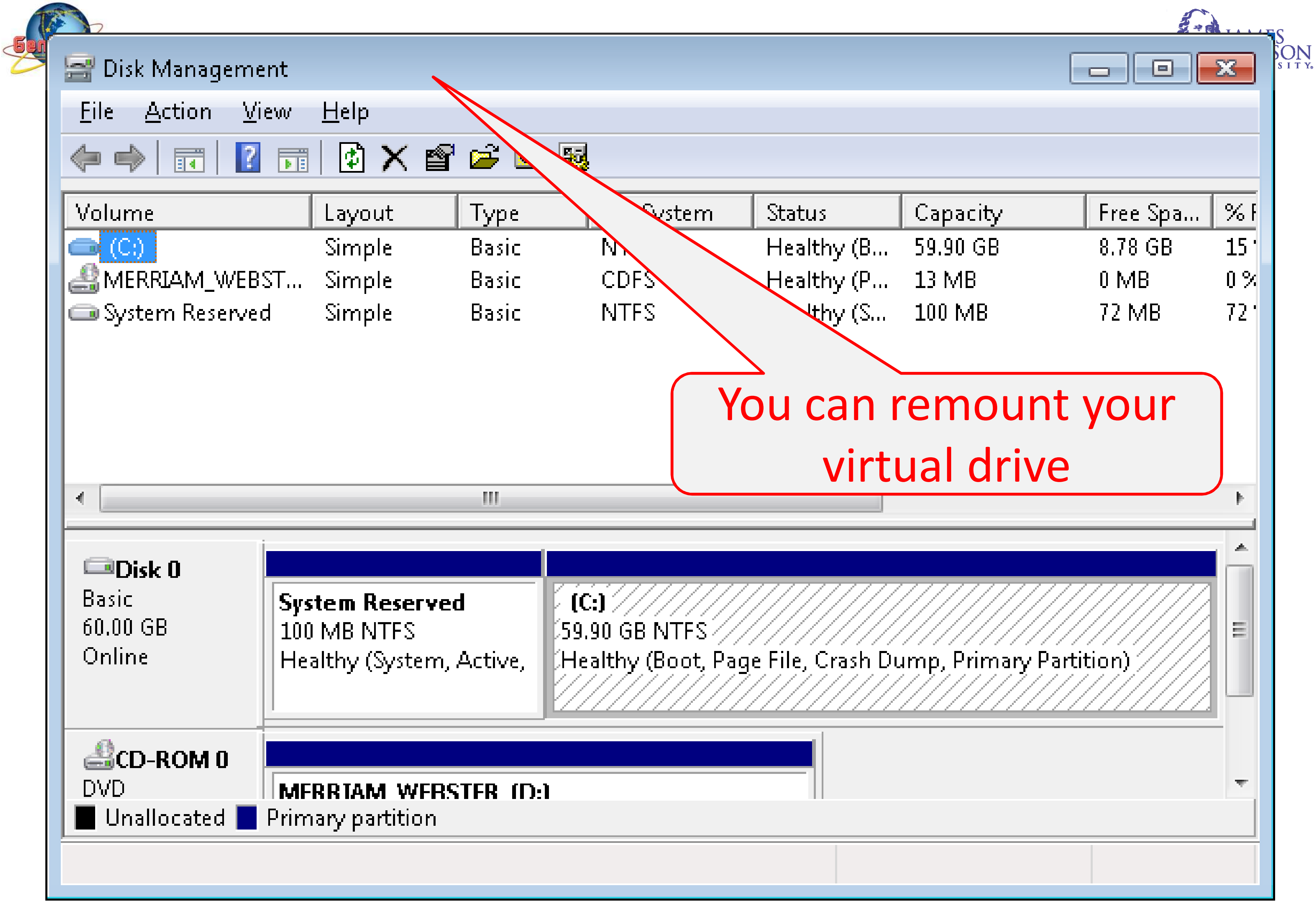
■ Unallocated ■ Primary partition

Disk 2 is gone (unmounted)



Name	Date modified	Type
bitlocker-test.vhd	11/30/2014 7:19 PM	VHD File
BitLocker Recovery Key 2723EF11-8 F-4...	11/30/2014 7:14 PM	Text Document
bitlocker-685.vhd	11/30/2014 6:40 PM	VHD File
20141130.txt	11/30/2014 3:37 PM	Text Document
2014-685-BitLocker Recovery Key C39CA...	0/2014 3:23 PM	Text Document
CryptoStat.html	1 14 9:14 AM	Chrome HTML Do...
Part09-Exploit writing tutorial...pdf	11/ 0:53 ...	PDF File
dropbox	11/30/ PM	File folder
2014-627-pdf	10/31/201	File folder
green	9/18/2014 1	e folder
457p2	9/1	
Web	9/1	

But your drive file IS still here



Volume	Layout	Type	System	Status	Capacity	Free Spa...	% F
(C:)	Simple	Basic	N	Healthy (B...	59.90 GB	8.78 GB	15
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %
System Reserved	Simple	Basic	NTFS	lthy (S...	100 MB	72 MB	72

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active,

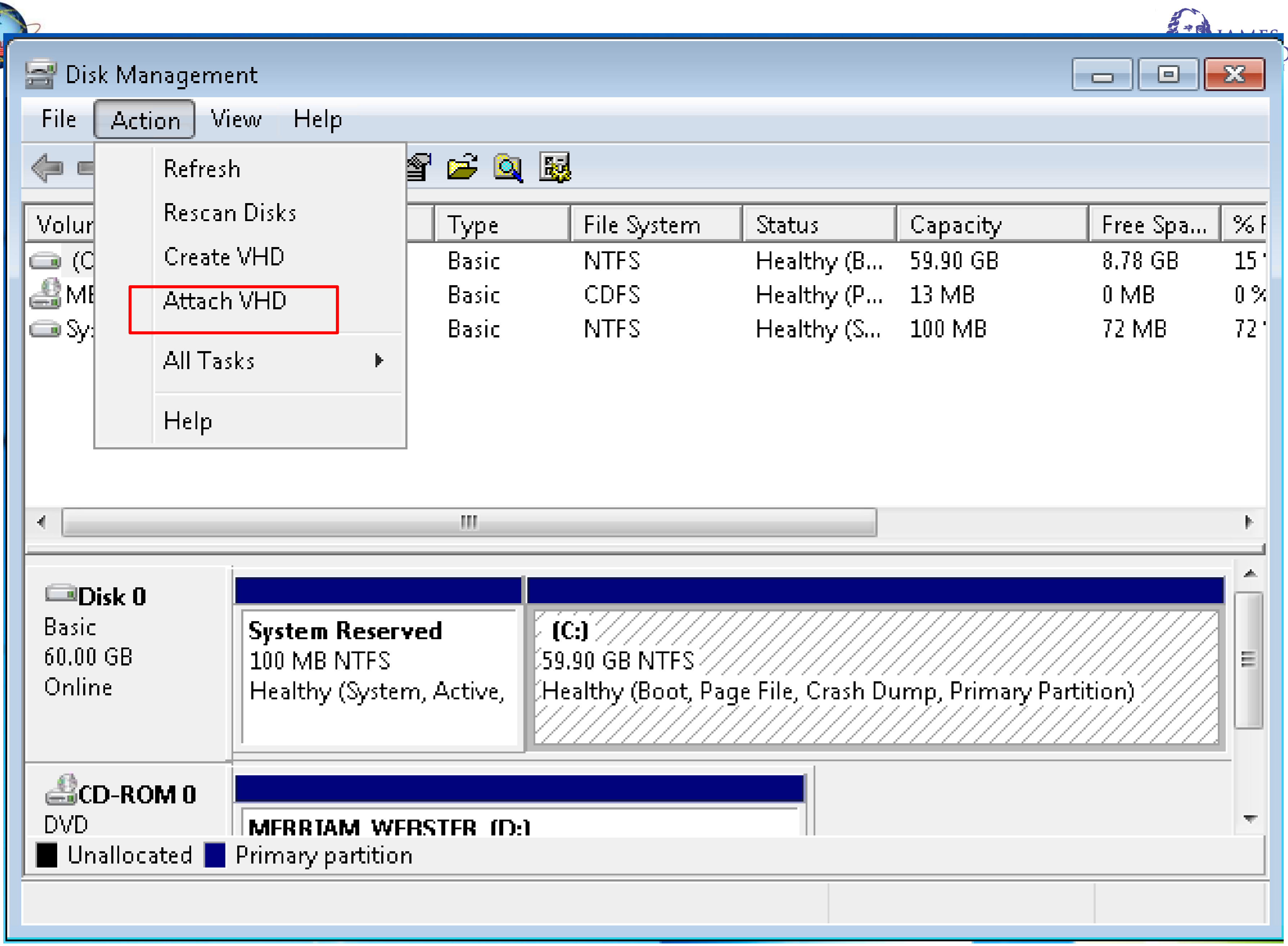
(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

CD-ROM 0
DVD

MERRIAM_WEBSTER (D:)

■ Unallocated ■ Primary partition

You can remount your virtual drive



Volur	Type	File System	Status	Capacity	Free Spa...	% F
(C	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15
ME	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %
Sy	Basic	NTFS	Healthy (S...	100 MB	72 MB	72

Disk 0
Basic
60.00 GB
Online

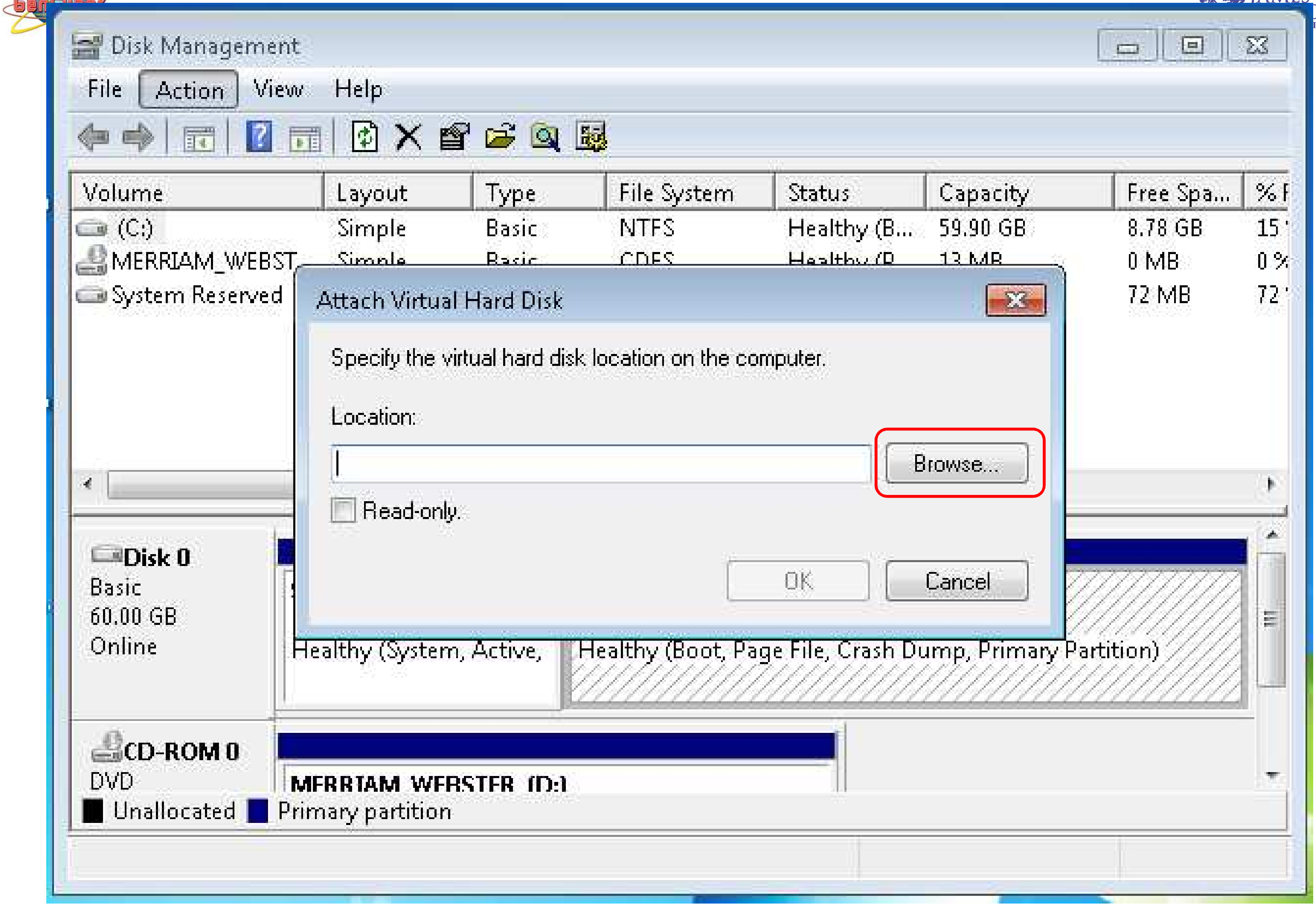
System Reserved
100 MB NTFS
Healthy (System, Active,

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

CD-ROM 0
DVD

MERRIAM_WEBSTER (D:)

■ Unallocated 🟦 Primary partition



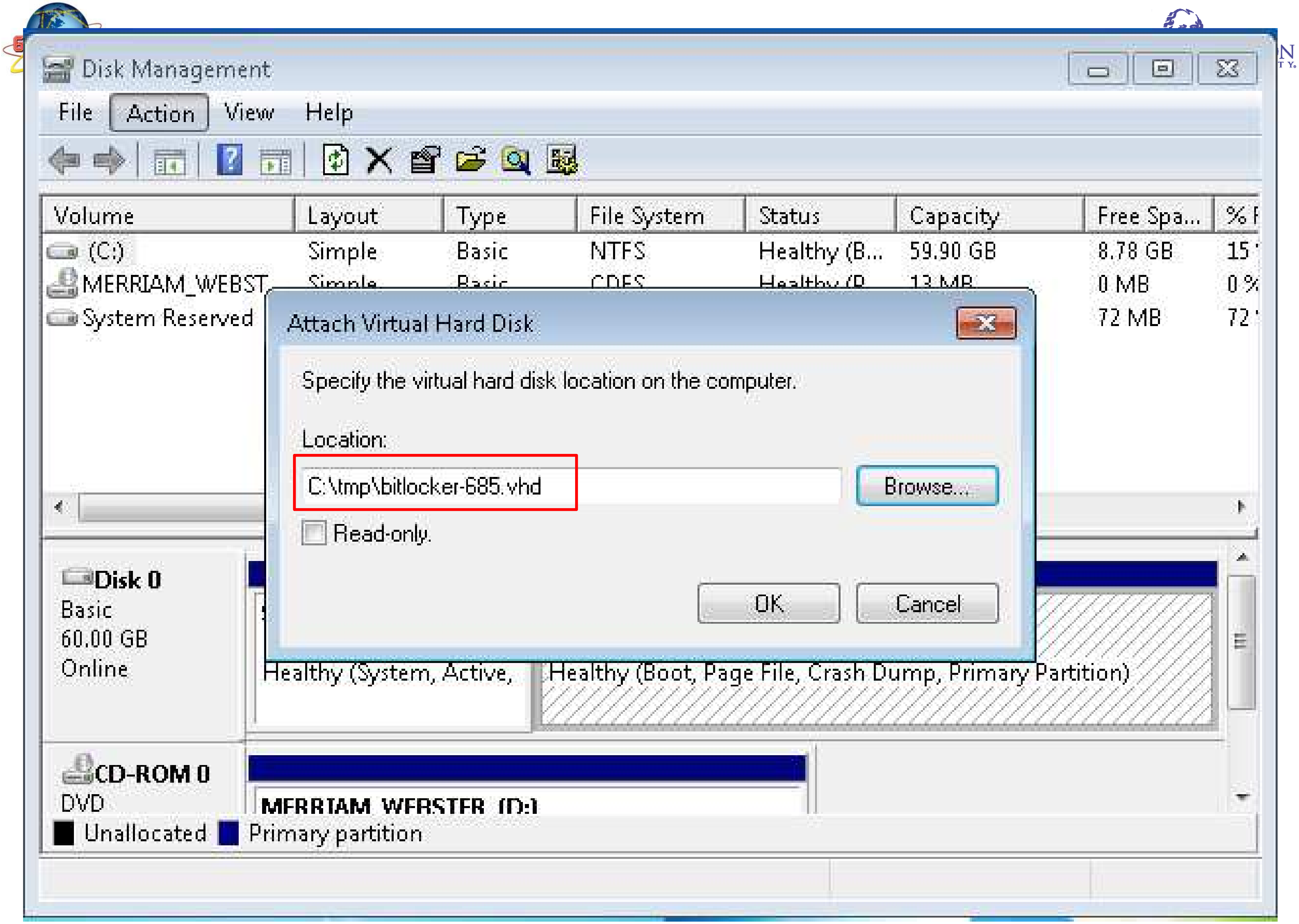
Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% F
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15
MERRIAM_WEBST	Simple	Basic	CDFS	Healthy (P	13 MB	0 MB	0 %
System Reserved						72 MB	72

Attach Virtual Hard Disk

Specify the virtual hard disk location on the computer.

Location:

□ Read-only.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% F
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15
MERRIAM_WEBST	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %
System Reserved						72 MB	72

Attach Virtual Hard Disk

Specify the virtual hard disk location on the computer.

Location:

C:\tmp\bitlocker-685.vhd

□ Read-only.

Disk 0
Basic
60.00 GB
Online

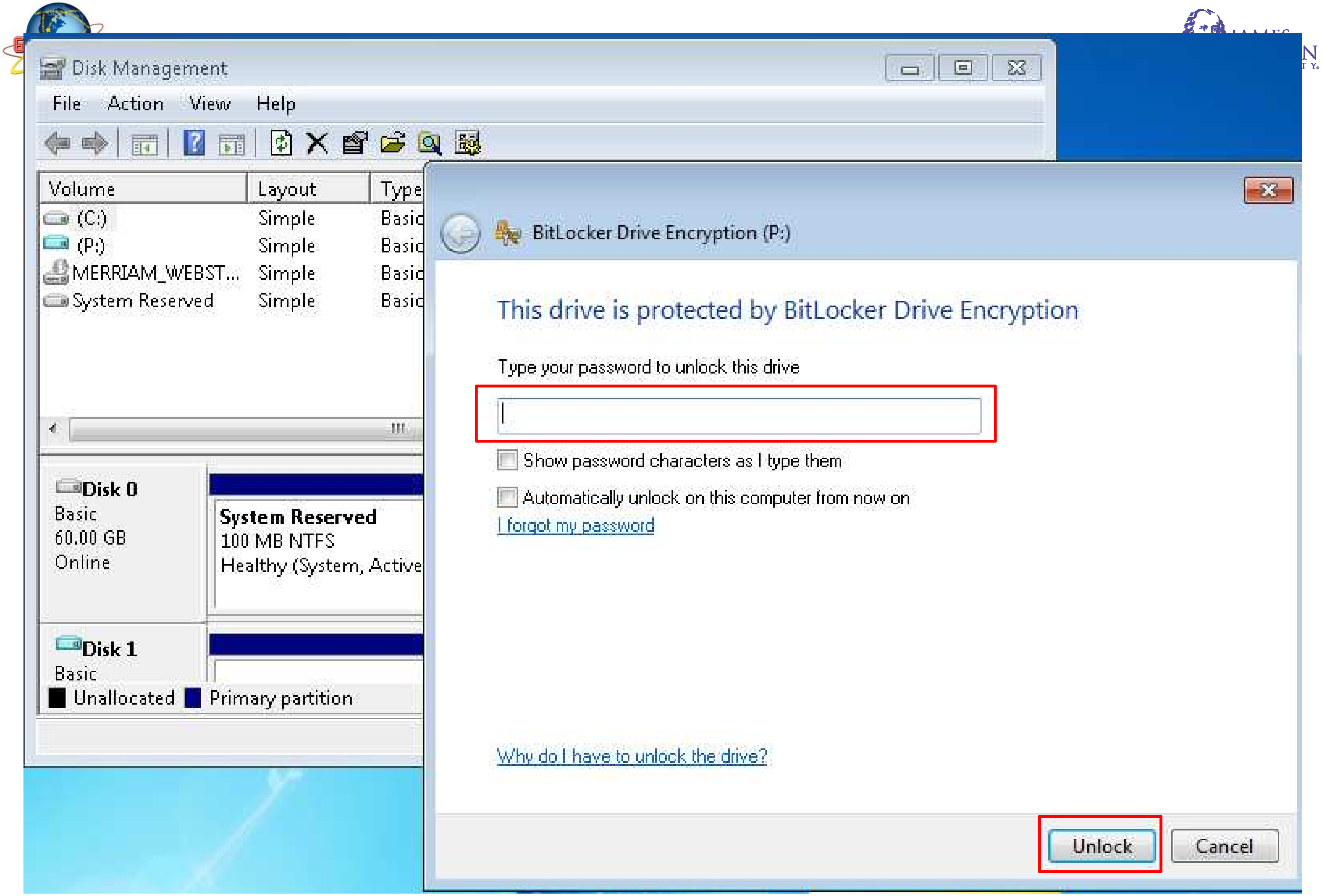
Healthy (System, Active,

Healthy (Boot, Page File, Crash Dump, Primary Partition)

CD-ROM 0
DVD

MERRIAM_WEBSTER (D:)

■ Unallocated ■ Primary partition



Volume	Layout	Type
(C:)	Simple	Basic
(P:)	Simple	Basic
MERRIAM_WEBST...	Simple	Basic
System Reserved	Simple	Basic

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active

Disk 1
Basic

■ Unallocated ■ Primary partition

BitLocker Drive Encryption (P:)

This drive is protected by BitLocker Drive Encryption

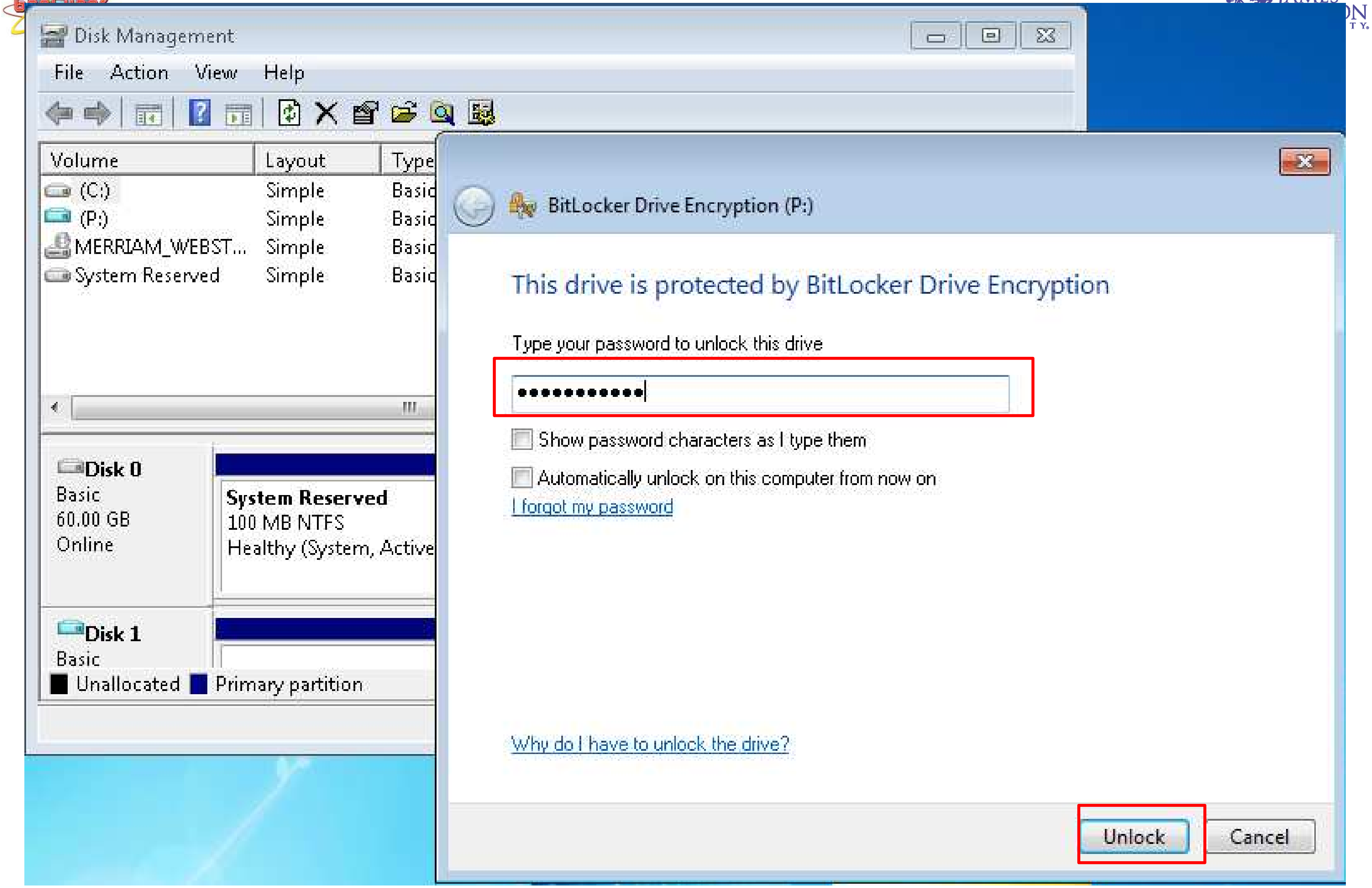
Type your password to unlock this drive

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?



Volume	Layout	Type
(C:)	Simple	Basic
(P:)	Simple	Basic
MERRIAM_WEBST...	Simple	Basic
System Reserved	Simple	Basic

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active

Disk 1
Basic

■ Unallocated ■ Primary partition

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

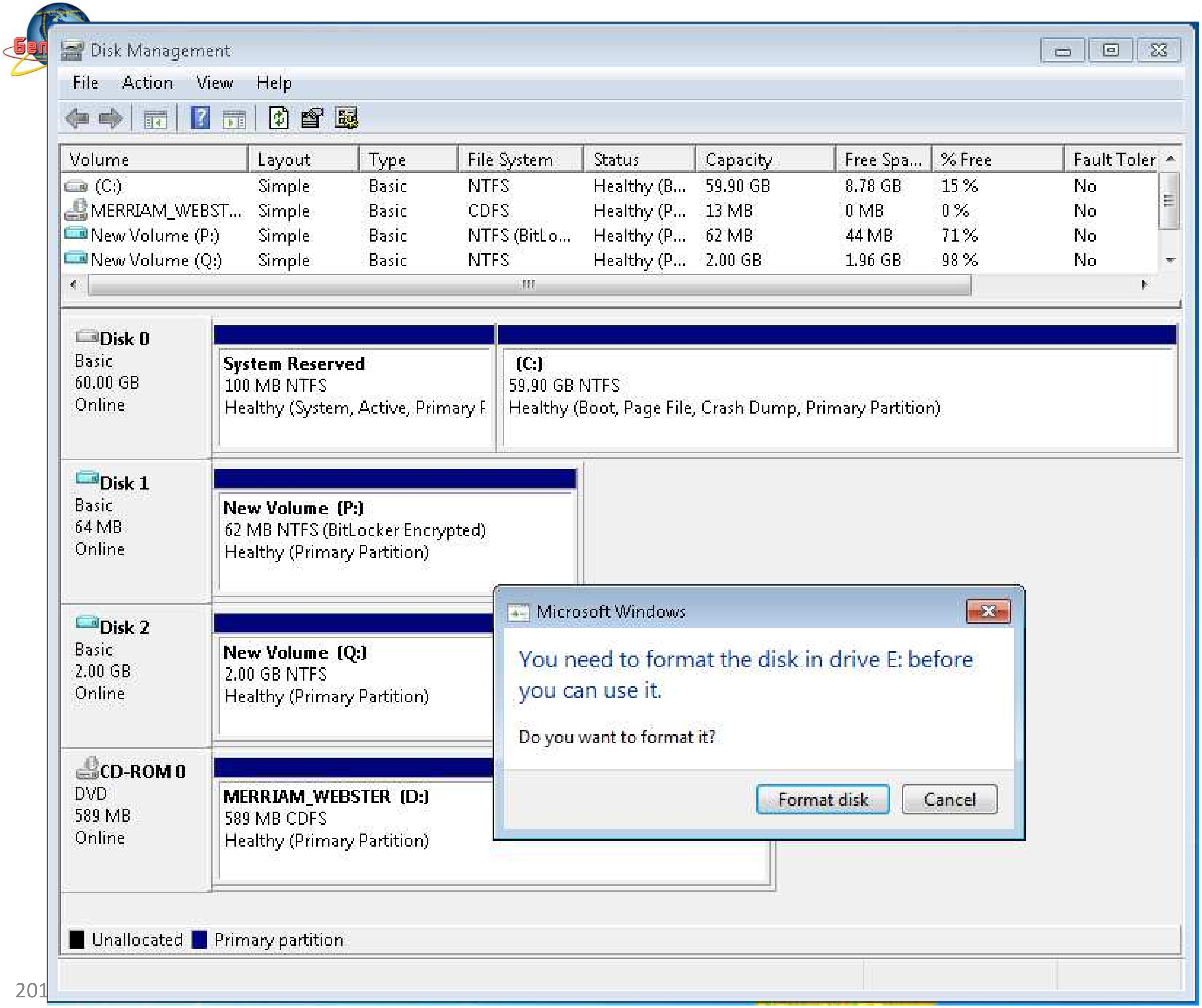
●●●●●●●●●●●●

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free	Fault Toler
(C:)	Simple	Basic	NTFS	Healthy (B...	59.90 GB	8.78 GB	15 %	No
MERRIAM_WEBST...	Simple	Basic	CDFS	Healthy (P...	13 MB	0 MB	0 %	No
New Volume (P:)	Simple	Basic	NTFS (BitLo...	Healthy (P...	62 MB	44 MB	71 %	No
New Volume (Q:)	Simple	Basic	NTFS	Healthy (P...	2.00 GB	1.96 GB	98 %	No

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active, Primary P

(C:)
59.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
64 MB
Online

New Volume (P:)
62 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

Disk 2
Basic
2.00 GB
Online

New Volume (Q:)
2.00 GB NTFS
Healthy (Primary Partition)

CD-ROM 0
DVD
589 MB
Online

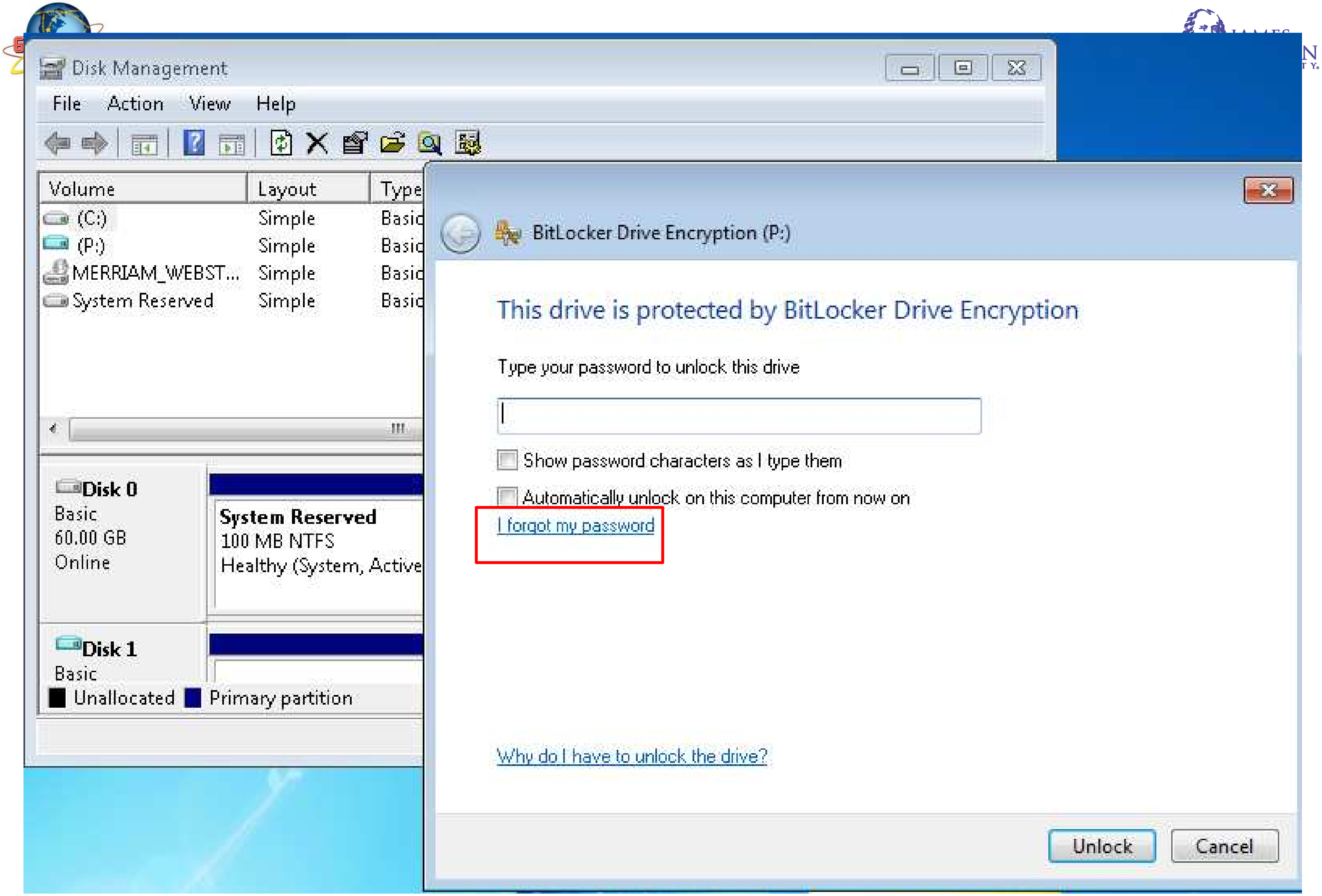
MERRIAM_WEBSTER (D:)
589 MB CDFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

Microsoft Windows

You need to format the disk in drive E: before you can use it.

Do you want to format it?



Volume	Layout	Type
(C:)	Simple	Basic
(P:)	Simple	Basic
MERRIAM_WEBST...	Simple	Basic
System Reserved	Simple	Basic

Disk 0
Basic
60.00 GB
Online

System Reserved
100 MB NTFS
Healthy (System, Active

Disk 1
Basic

■ Unallocated ■ Primary partition

BitLocker Drive Encryption (P:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?

Summary

- Practice
  - Truecrypt
  - GPG
  - BitLocker