The Higher Education Academy

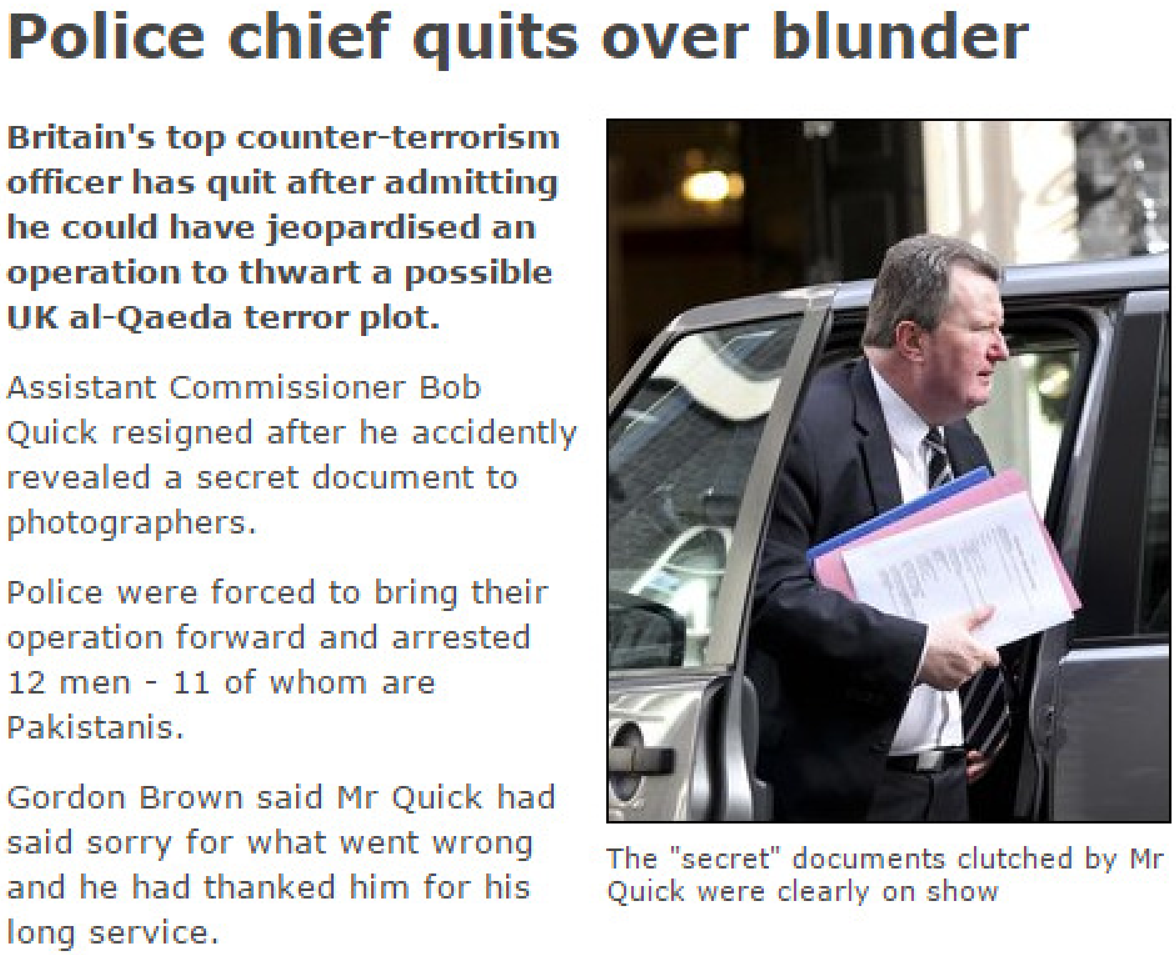
BIRMINGHAM CITY University

Digital Evidence Management System

Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

An illustration …



Police chief quits over blunder

Britain's top counter-terrorism officer has quit after admitting he could have jeopardised an operation to thwart a possible UK al-Qaeda terror plot.

Assistant Commissioner Bob Quick resigned after he accidently revealed a secret document to photographers.

Police were forced to bring their operation forward and arrested 12 men - 11 of whom are Pakistanis.

Gordon Brown said Mr Quick had said sorry for what went wrong and he had thanked him for his long service.

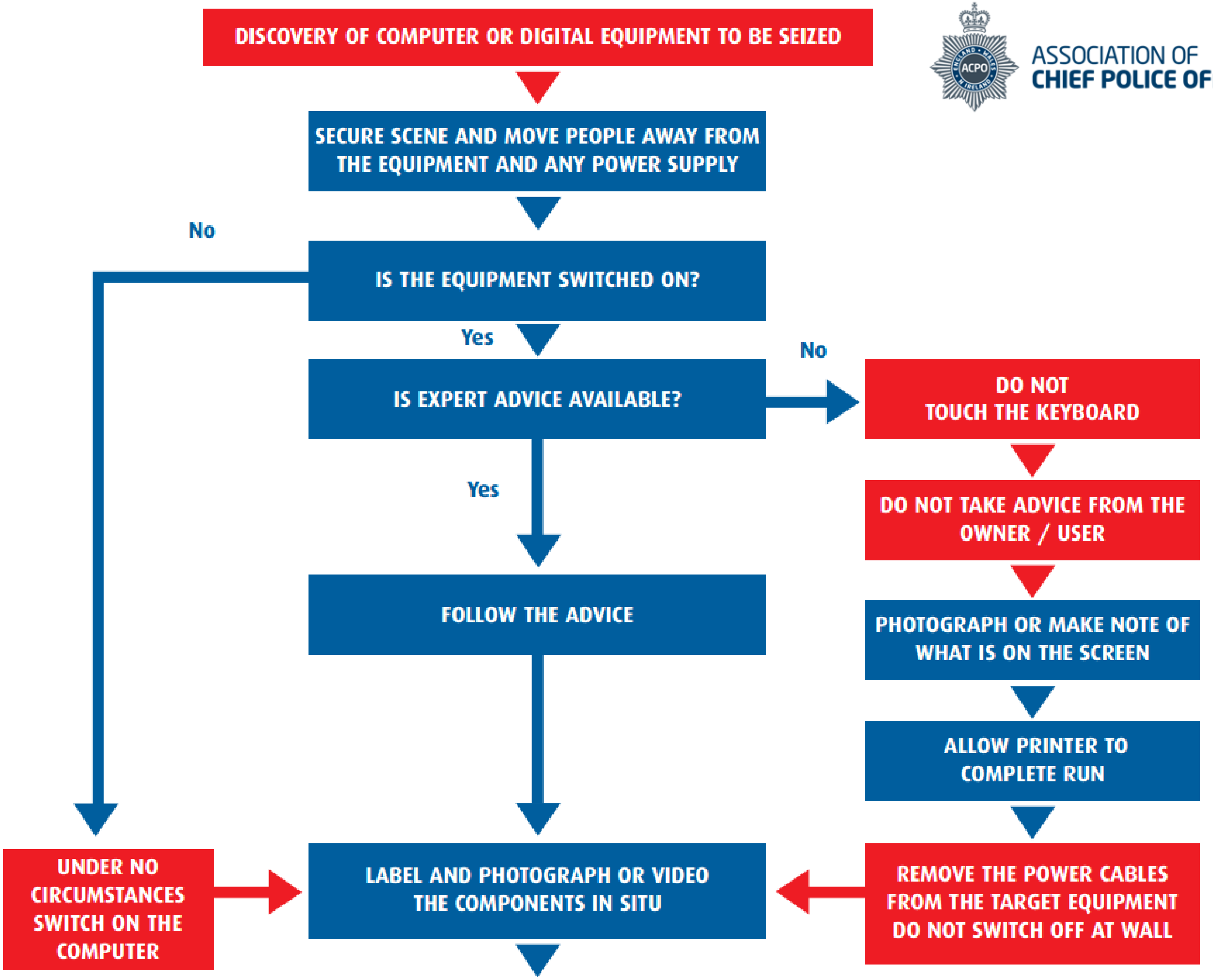
The "secret" documents clutched by Mr Quick were clearly on show

BIRMINGHAM CITY University

Who am I ?

- Lecturer in Digital Forensics at Birmingham City University
- Vice-President/Board Member of ISSA (Information Systems Security Association) Brussels European Chapter
- Past activities
  - Senior Consultant at "Forensic Technology Solutions" of PricewaterhouseCoopers Enterprise Advisory
  - Co-chair of NESSI-TSD (Networked European Software and Services Initiative – Trust, Security & Dependability Working Group)

ASSOCIATION OF
CHIEF POLICE OFFICERS



DISCOVERY OF COMPUTER OR DIGITAL EQUIPMENT TO BE SEIZED

SECURE SCENE AND MOVE PEOPLE AWAY FROM THE EQUIPMENT AND ANY POWER SUPPLY

IS THE EQUIPMENT SWITCHED ON?

No

Yes

IS EXPERT ADVICE AVAILABLE?

No

DO NOT TOUCH THE KEYBOARD

DO NOT TAKE ADVICE FROM THE OWNER / USER

PHOTOGRAPH OR MAKE NOTE OF WHAT IS ON THE SCREEN

ALLOW PRINTER TO COMPLETE RUN

REMOVE THE POWER CABLES FROM THE TARGET EQUIPMENT DO NOT SWITCH OFF AT WALL

Yes

FOLLOW THE ADVICE

UNDER NO CIRCUMSTANCES SWITCH ON THE COMPUTER

LABEL AND PHOTOGRAPH OR VIDEO THE COMPONENTS IN SITU

ASSOCIATION OF
CHIEF POLICE OFFICERS

BIRMINGHAM CITY
University

Transport

Handle all equipment with care

Keep all equipment away from magnetic sources such as loudspeakers, heated seats / windows or police radios

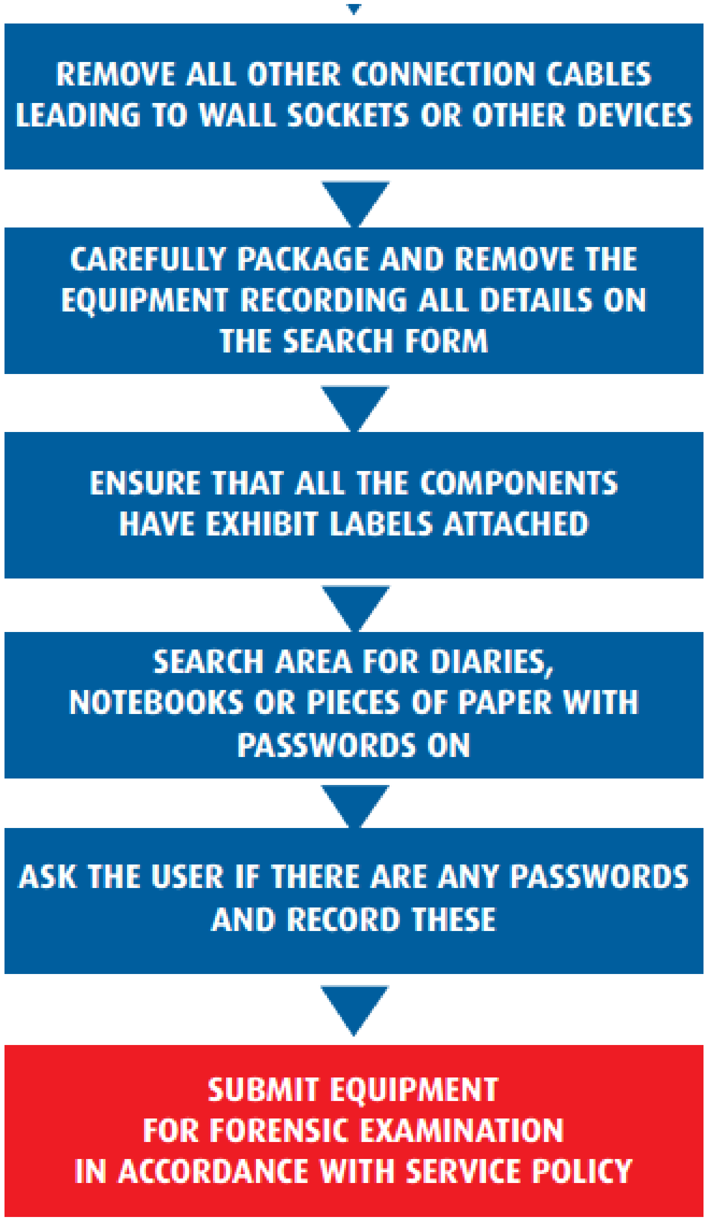
Place hard disks and circuit boards in anti-static bags

Do not bend floppy disks or place labels directly on them

Transport monitors face down on the back seat of car (belted in)

Place personal organisers and palmtop computers in paper envelopes

Place keyboards, leads, mouse and modems in aerated bags. Do not place under heavy objects.



REMOVE ALL OTHER CONNECTION CABLES LEADING TO WALL SOCKETS OR OTHER DEVICES

CAREFULLY PACKAGE AND REMOVE THE EQUIPMENT RECORDING ALL DETAILS ON THE SEARCH FORM

ENSURE THAT ALL THE COMPONENTS HAVE EXHIBIT LABELS ATTACHED

SEARCH AREA FOR DIARIES, NOTEBOOKS OR PIECES OF PAPER WITH PASSWORDS ON

ASK THE USER IF THERE ARE ANY PASSWORDS AND RECORD THESE

SUBMIT EQUIPMENT FOR FORENSIC EXAMINATION IN ACCORDANCE WITH SERVICE POLICY

What should be seized

For reconstruction of the system:
Main Unit - usually the box to which the keyboard and monitor are attached
Monitor
Keyboard and mouse
All leads (including power cables)
Power Supply Units
Hard Disks - not fitted inside the computer
Dongles (small connectors plugged into the back of the machine, usually in socket marked PRINTER or LPT1)
Modems (some contain phone numbers)

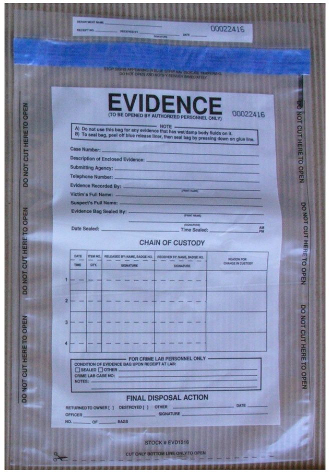
For retrieval of evidence:
Floppy Disks, CDs, DAT Tapes, Jaz cartridges and ZIP cartridges
PCMCIA cards
Hard Disks not connected to the computer

To assist with the examination:

Manuals and computer software
Paper with passwords on
Keys

For comparison of printouts:
Printers
Printouts and Printer paper

Collection and Preservation



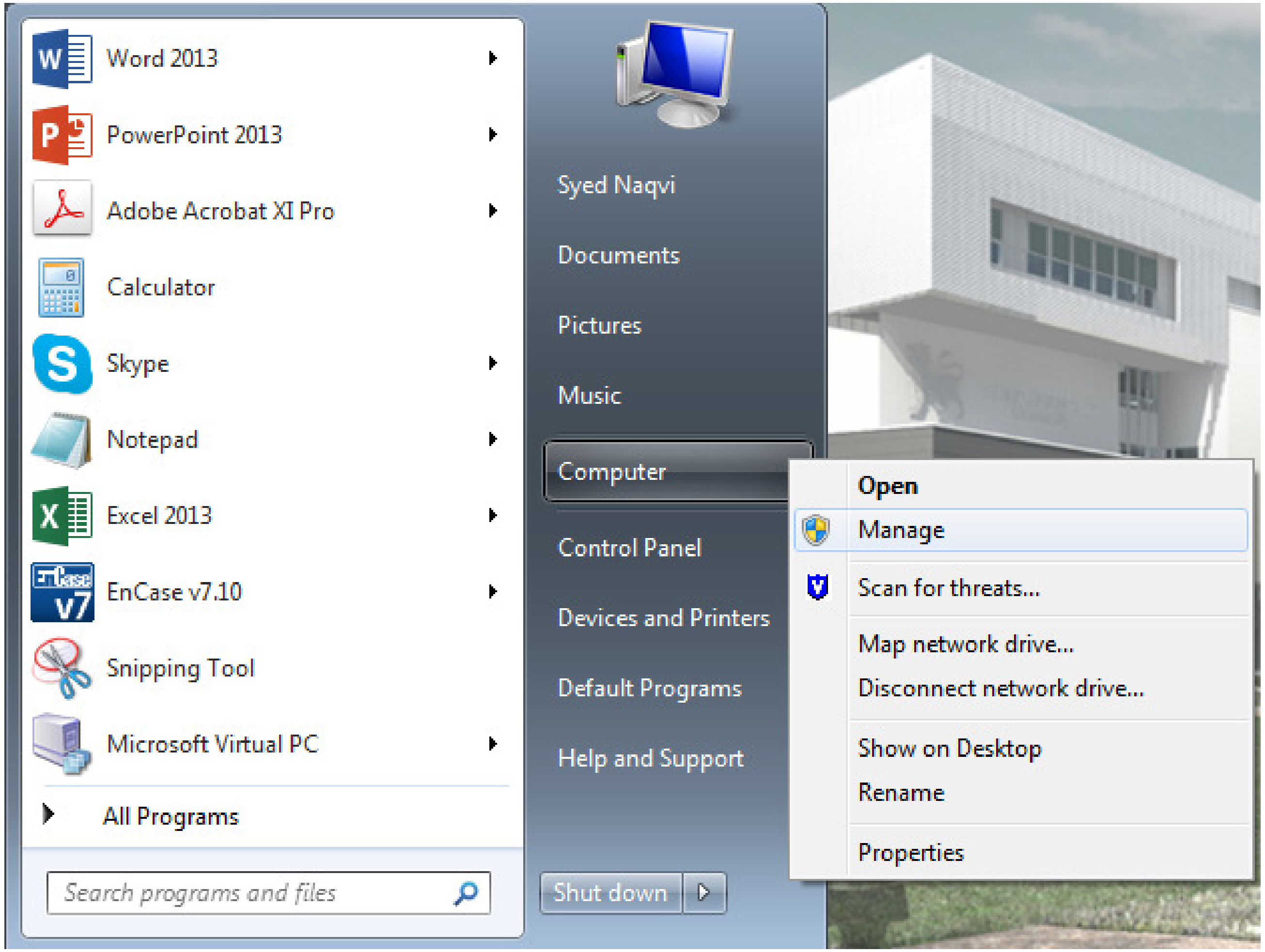
Encrypted Containers

http://pcuserinfo.com/wp-content/uploads/2011/11/data-encryption_300.jpg

Exercise

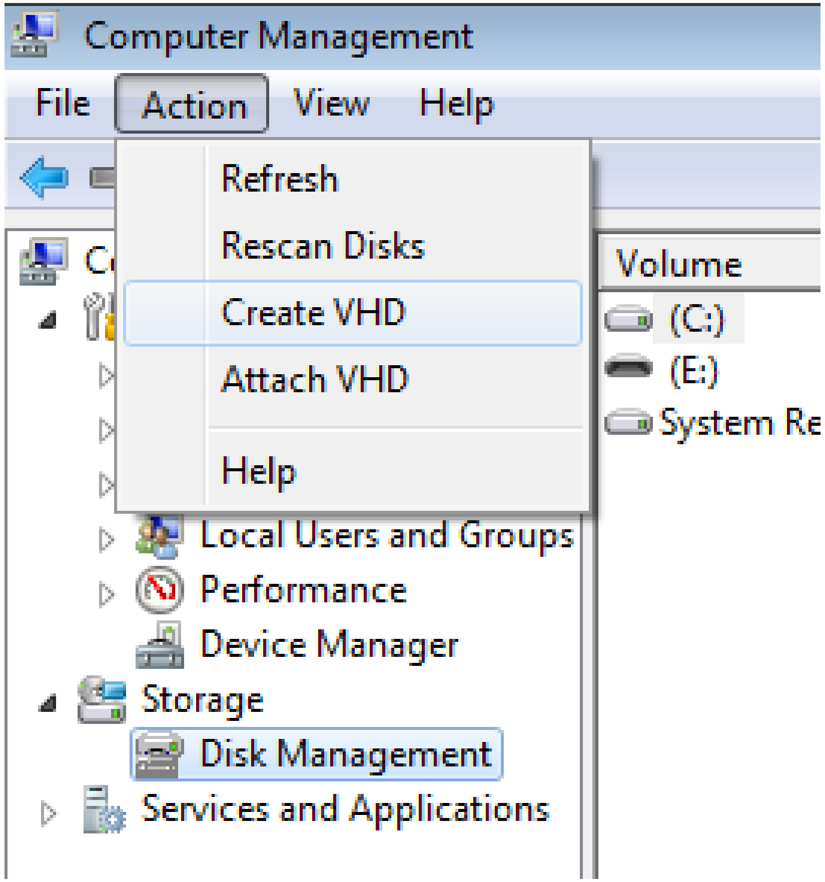
http://mk-dizajn.com/wp-content/uploads/2014/06/data-encryption.jpg

Run Disk Management Tool

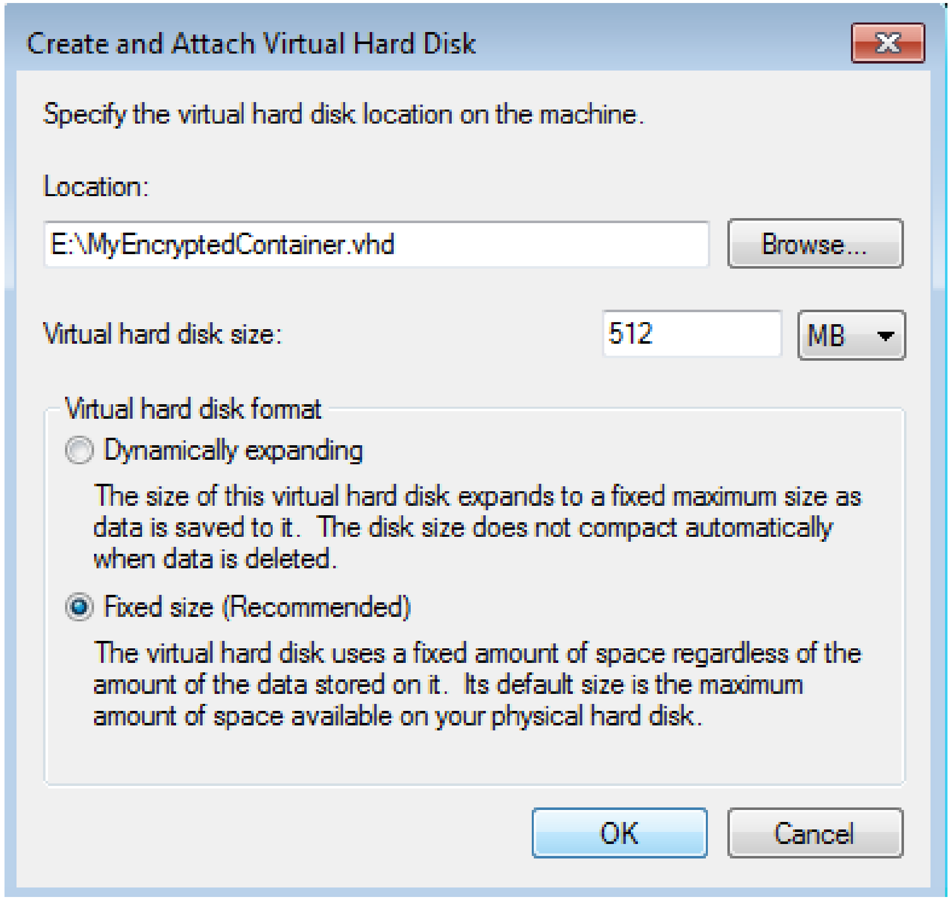


BIRMINGHAM CITY University

Create a Virtual Hard Drive File



Create a Virtual Hard Drive File



Create and Attach Virtual Hard Disk

Specify the virtual hard disk location on the machine.

Location: E:\MyEncryptedContainer.vhd

Virtual hard disk size: 512 MB

Virtual hard disk format

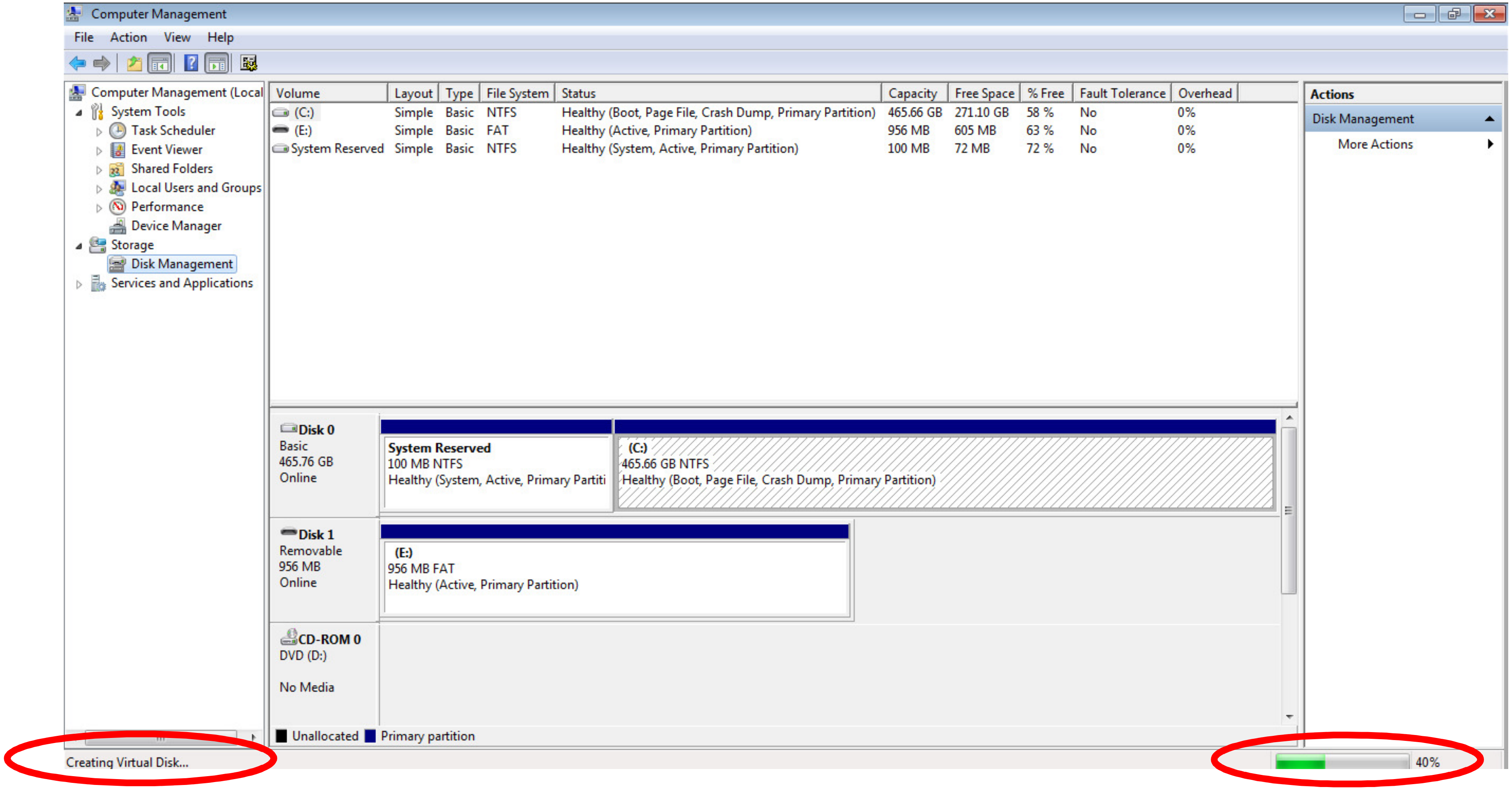
○ Dynamically expanding

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.

Create a Virtual Hard Drive File



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	465.66 GB	271.10 GB	58 %	No	0%
(E:)	Simple	Basic	FAT	Healthy (Active, Primary Partition)	956 MB	605 MB	63 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	72 MB	72 %	No	0%

Disk 0
Basic
465.76 GB
Online

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

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

Disk 1
Removable
956 MB
Online

(E:)
956 MB FAT
Healthy (Active, Primary Partition)

CD-ROM 0
DVD (D:)

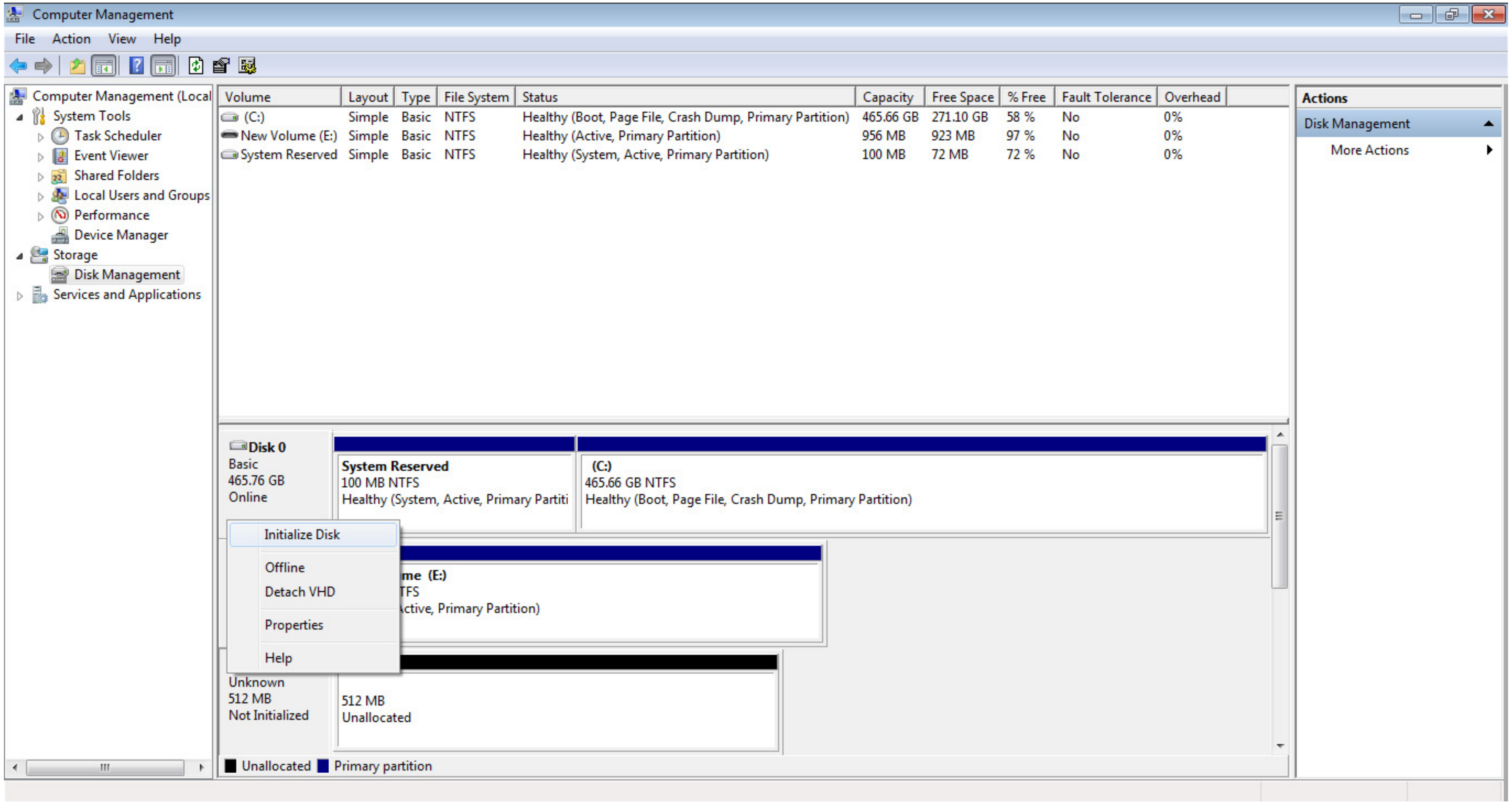
No Media

■ Unallocated ■ Primary partition

Creating Virtual Disk...

40%

Create a Virtual Hard Drive File



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	465.66 GB	271.10 GB	58 %	No	0%
New Volume (E:)	Simple	Basic	NTFS	Healthy (Active, Primary Partition)	956 MB	923 MB	97 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	72 MB	72 %	No	0%

Disk 0
Basic
465.76 GB
Online

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

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

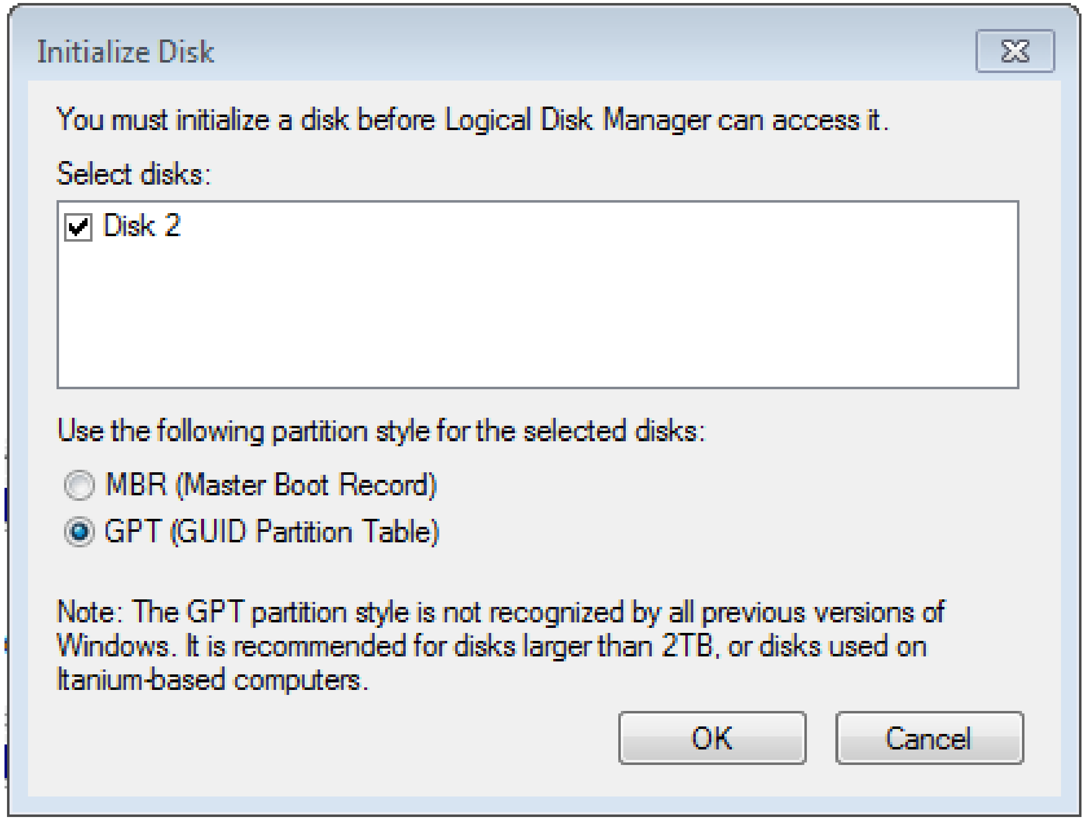
me (E:)
TFS
ctive, Primary Partition)

Unknown
512 MB
Not Initialized

512 MB
Unallocated

■ Unallocated ■ Primary partition

Create a Virtual Hard Drive File



Initialize Disk

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

Select disks:

☑ Disk 2

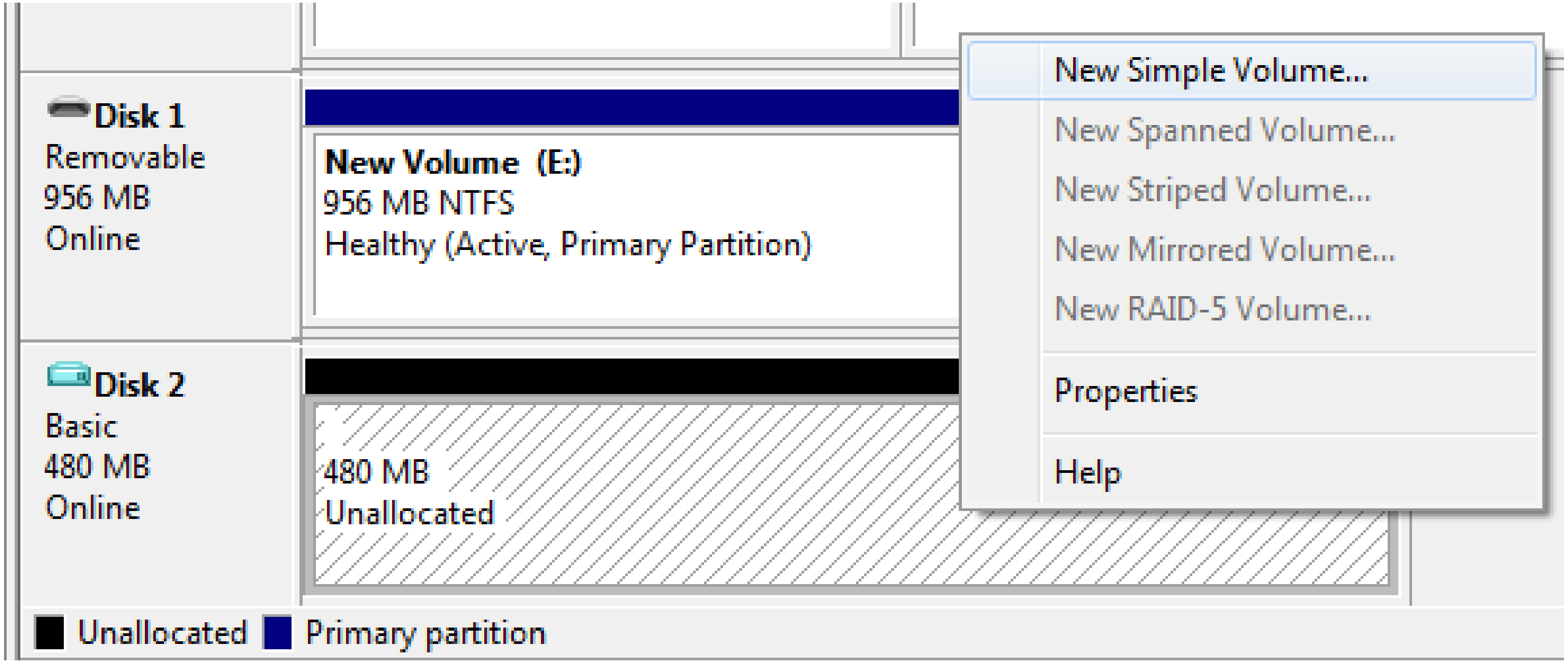
Use the following partition style for the selected disks:

○ 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.

Create a Virtual Hard Drive File



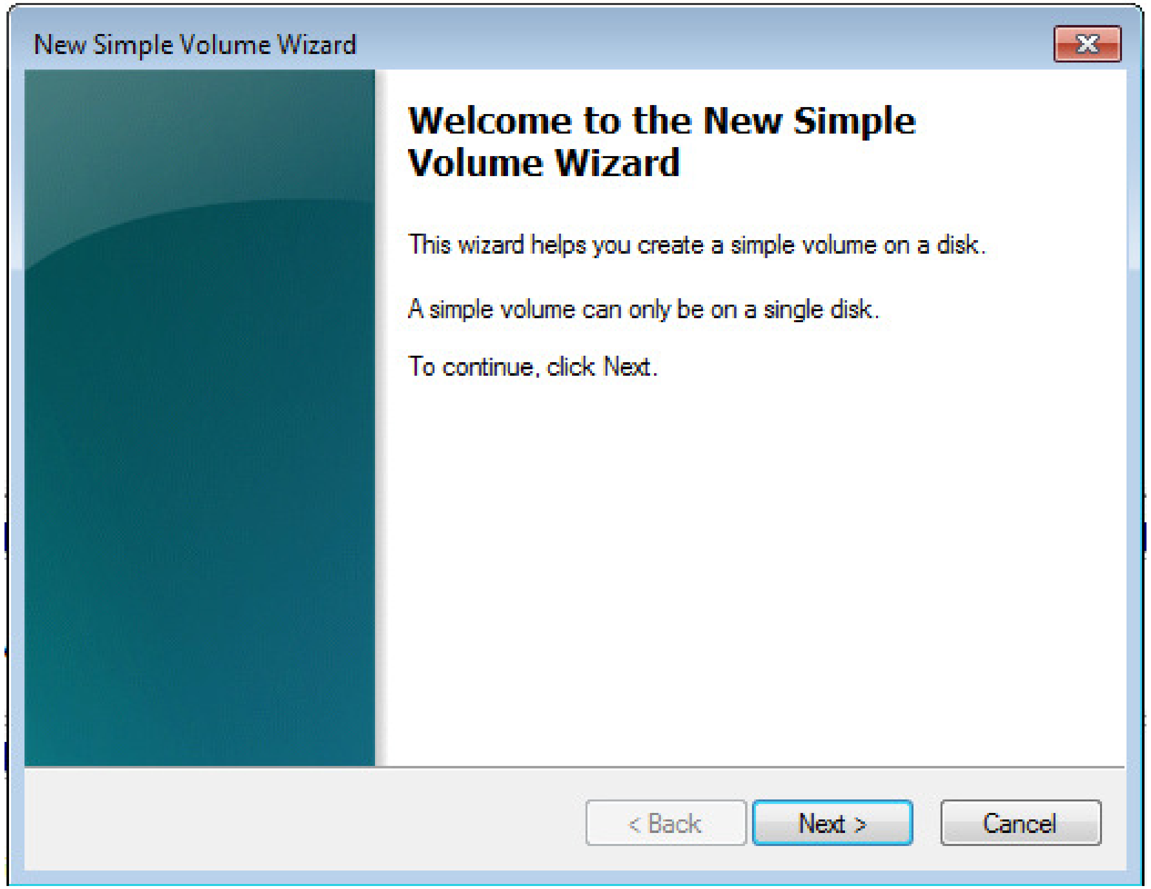
Disk 1
Removable
956 MB
Online

New Volume (E:)
956 MB NTFS
Healthy (Active, Primary Partition)

Disk 2
Basic
480 MB
Online

480 MB
Unallocated

Create a Virtual Hard Drive File



Welcome to the New Simple Volume Wizard

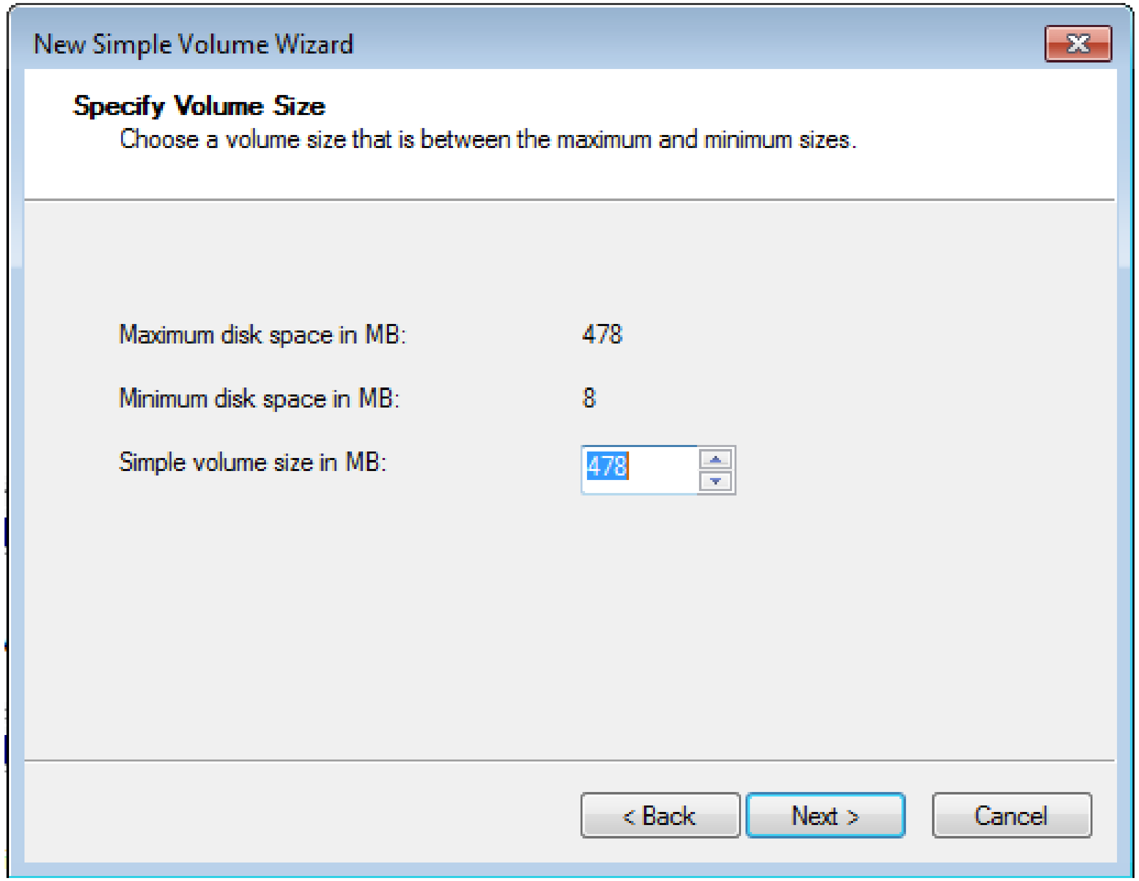
This wizard helps you create a simple volume on a disk.

A simple volume can only be on a single disk.

To continue, click Next.

BIRMINGHAM CITY University

Create a Virtual Hard Drive File



New Simple Volume Wizard

Specify Volume Size

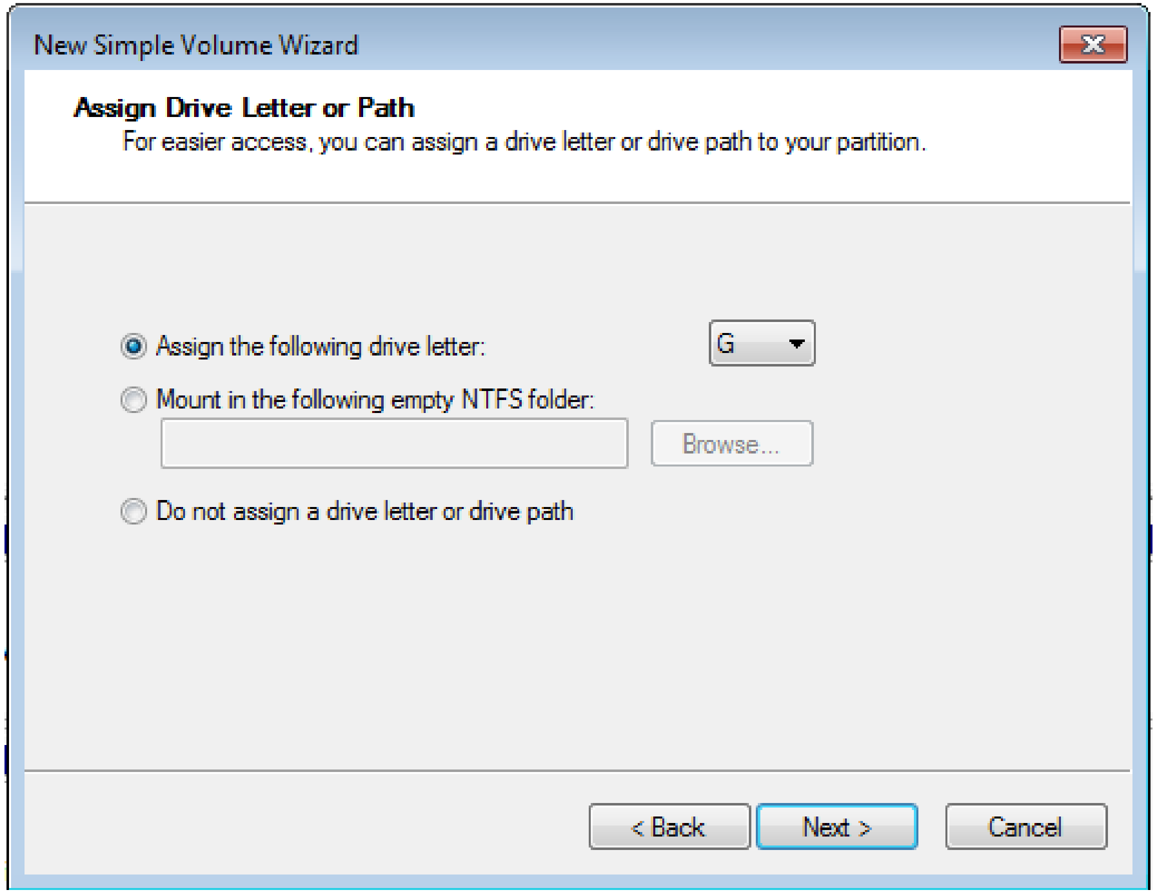
Choose a volume size that is between the maximum and minimum sizes.

Maximum disk space in MB: 478

Minimum disk space in MB: 8

Simple volume size in MB: 478

Create a Virtual Hard Drive File



New Simple Volume Wizard

Assign Drive Letter or Path

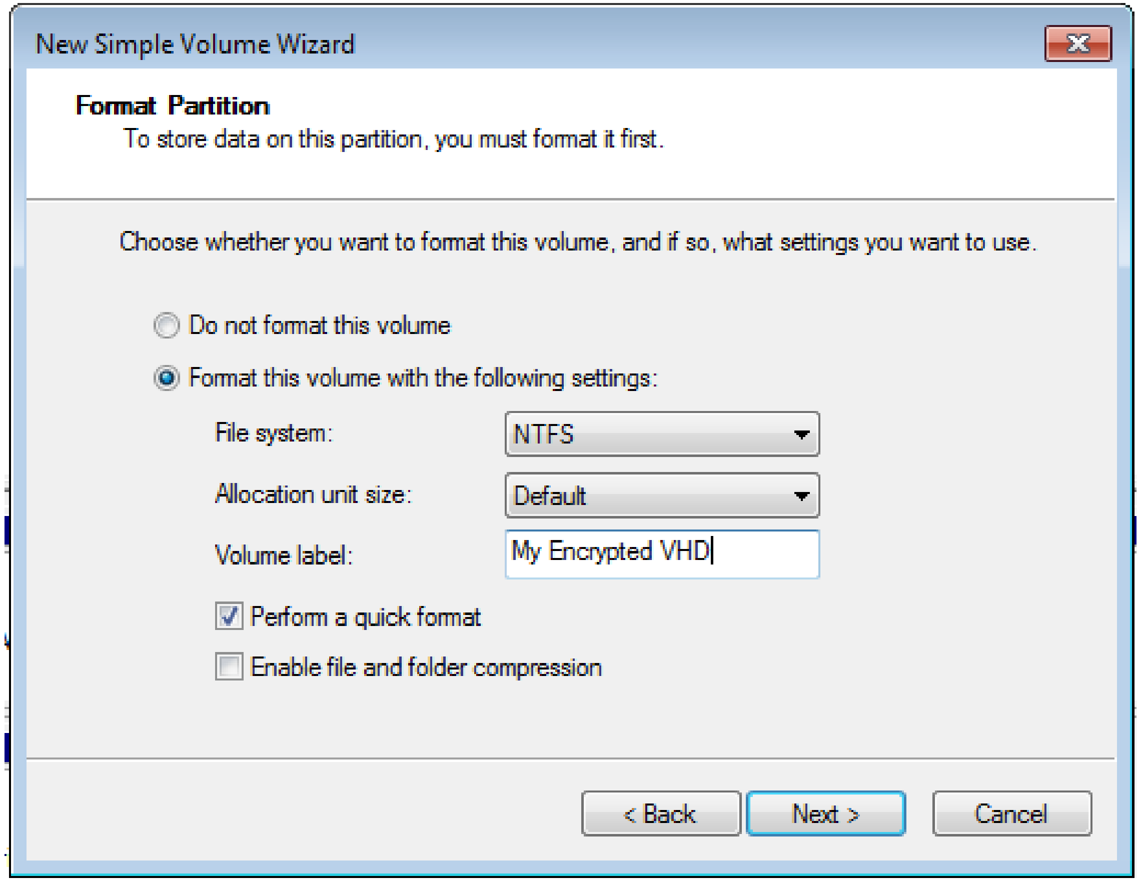
For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: G

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

Create a Virtual Hard Drive File



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

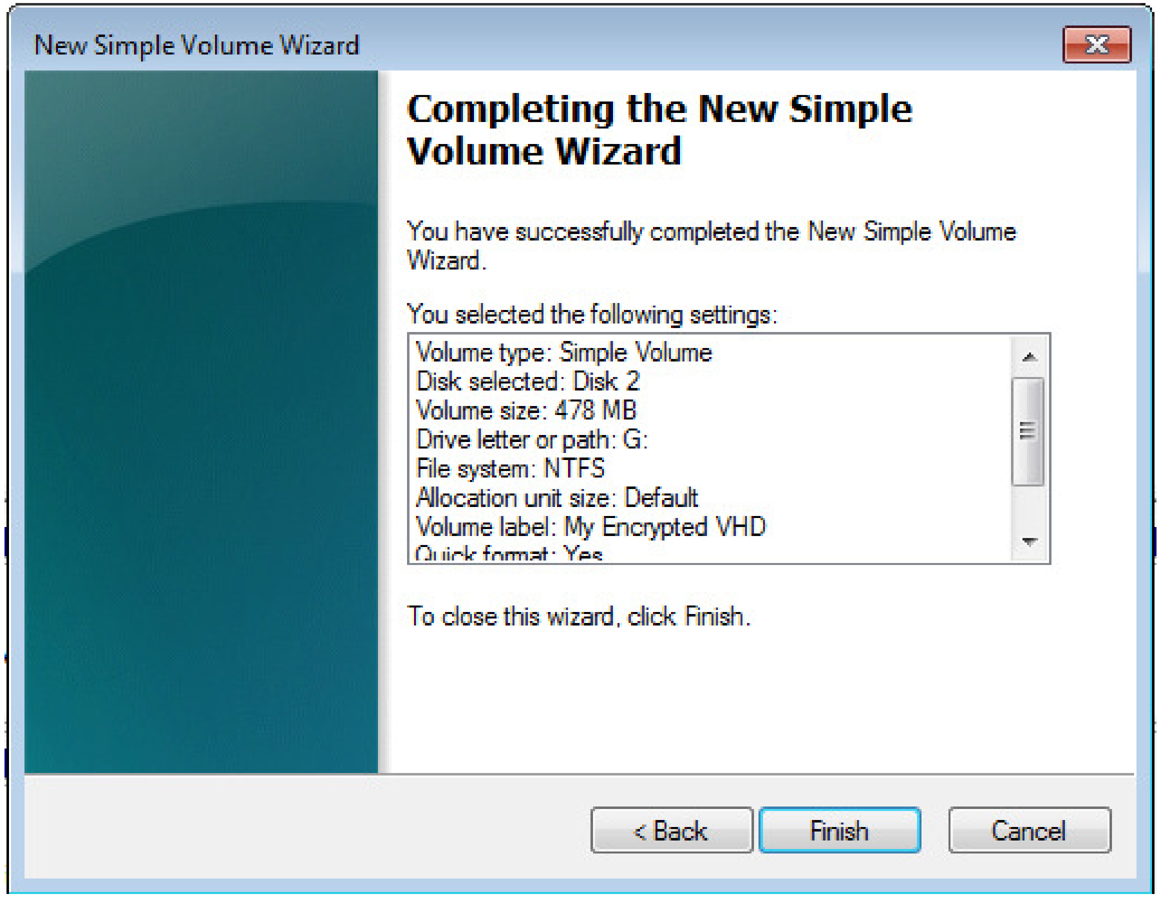
Allocation unit size: Default

Volume label: My Encrypted VHD

☑ Perform a quick format

□ Enable file and folder compression

Create a Virtual Hard Drive File



Completing the New Simple Volume Wizard

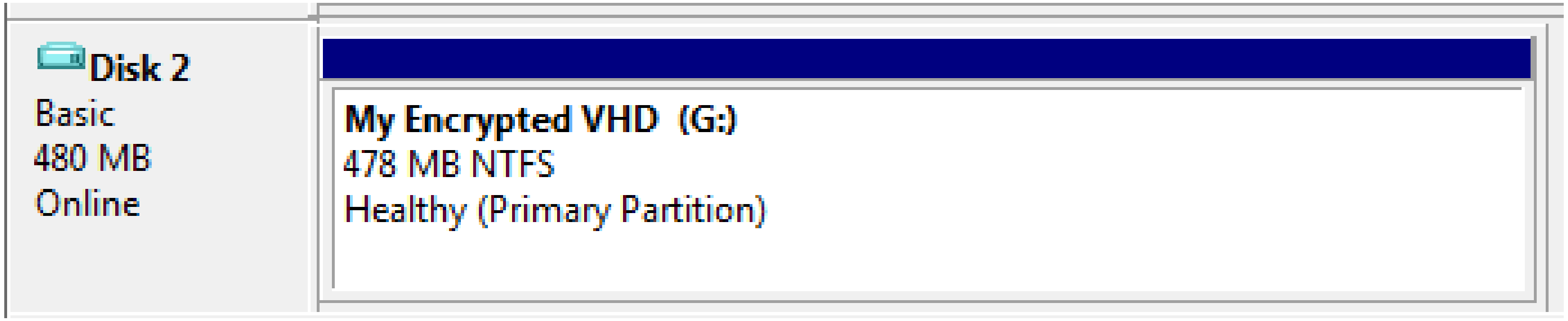
You have successfully completed the New Simple Volume Wizard.

You selected the following settings:

```
Volume type: Simple Volume
Disk selected: Disk 2
Volume size: 478 MB
Drive letter or path: G:
File system: NTFS
Allocation unit size: Default
Volume label: My Encrypted VHD
Quick format: Yes
```

To close this wizard, click Finish.

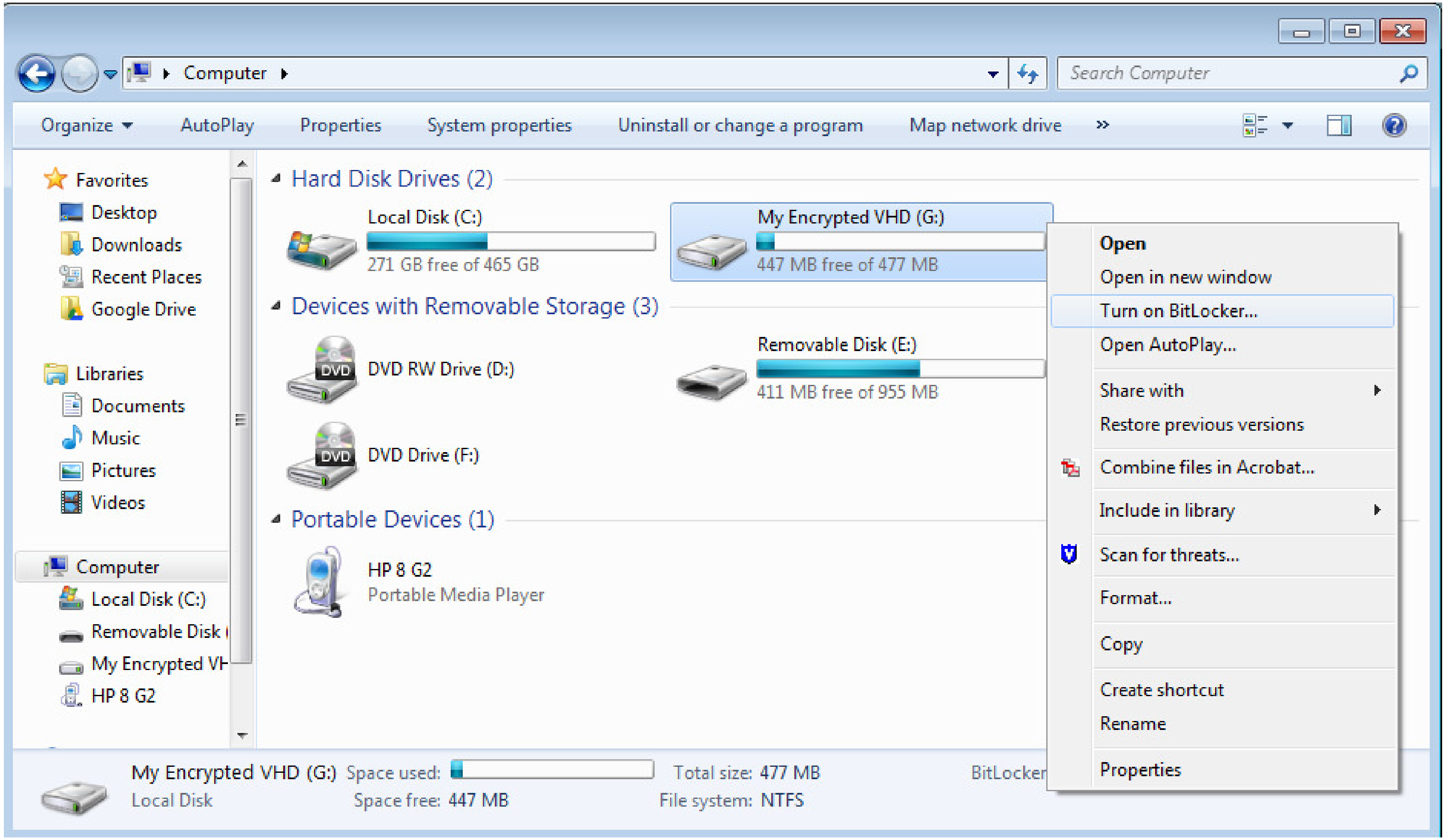
Create a Virtual Hard Drive File



Disk 2
Basic
480 MB
Online

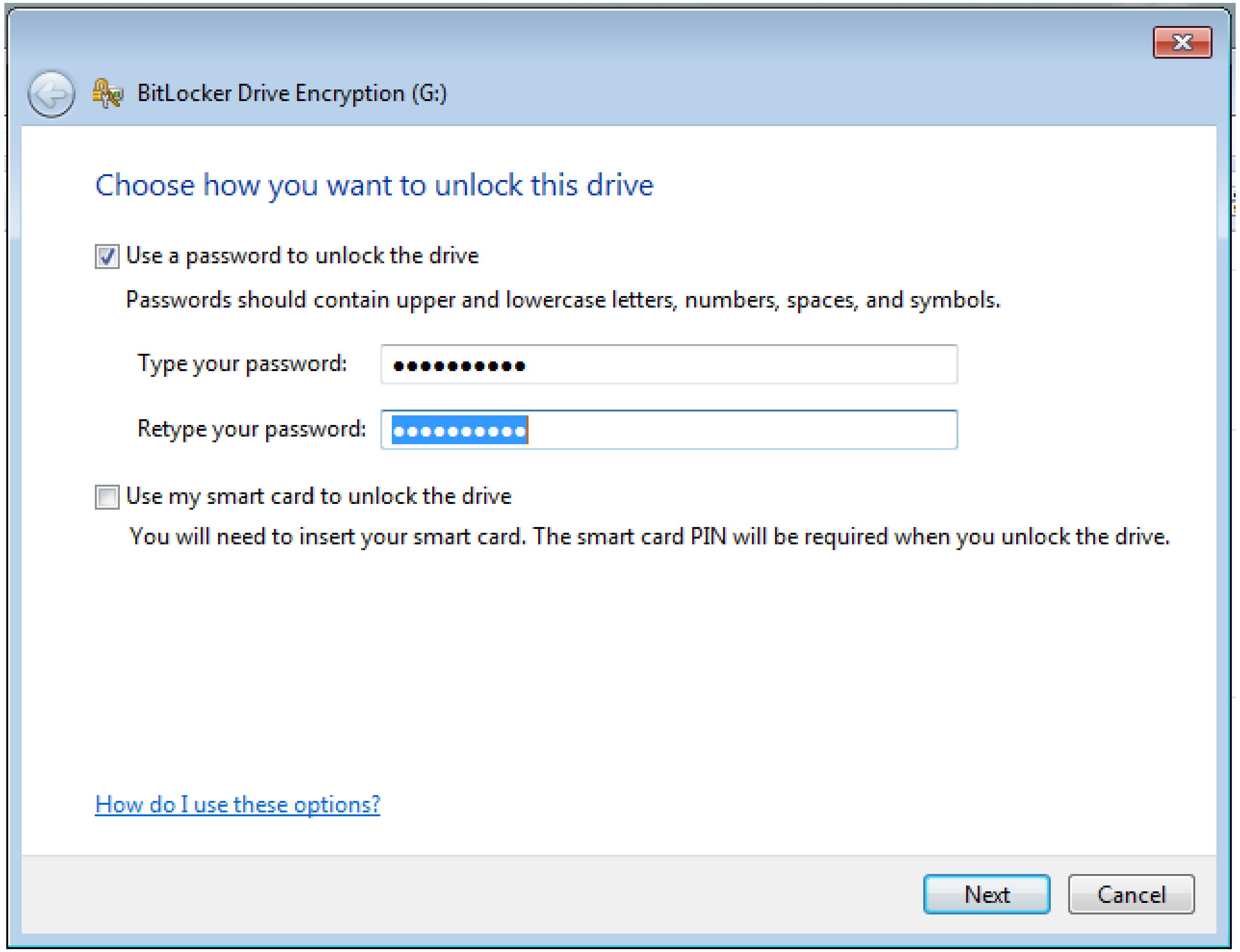
My Encrypted VHD (G:)
478 MB NTFS
Healthy (Primary Partition)

Encrypt the Disk Image



My Encrypted VHD (G:) Space used: Total size: 477 MB
Local Disk Space free: 447 MB File system: NTFS

Encrypt the Disk Image



BitLocker Drive Encryption (G:)

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: ●●●●●●●●●●●

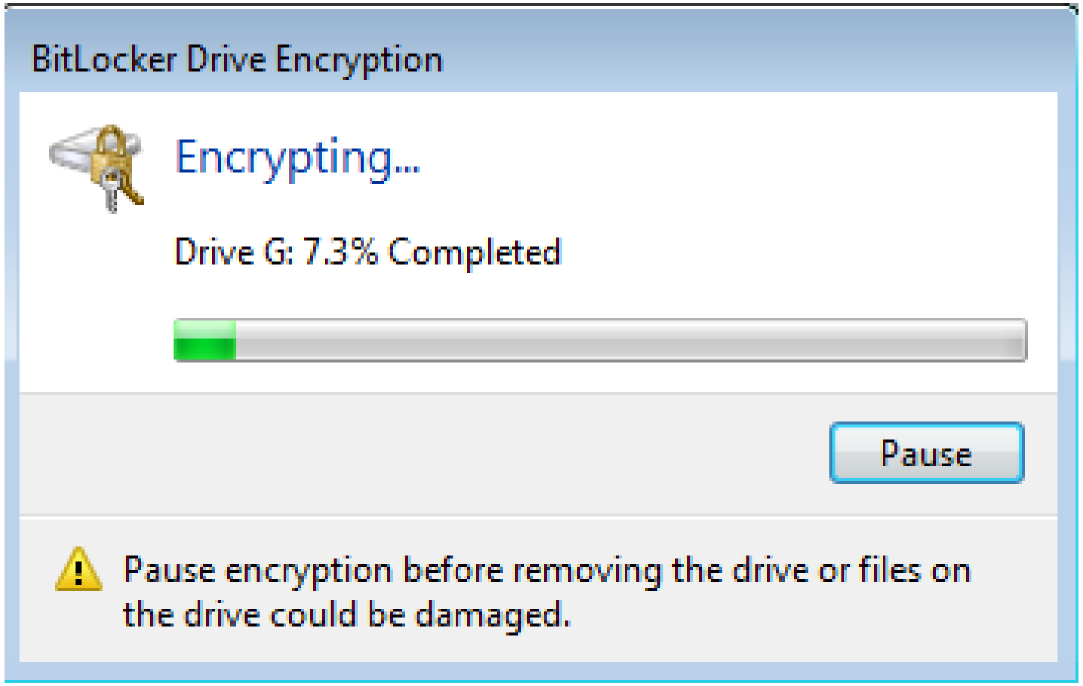
Retype your password: ●●●●●●●●●●●

□ 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?

Encrypt the Disk Image



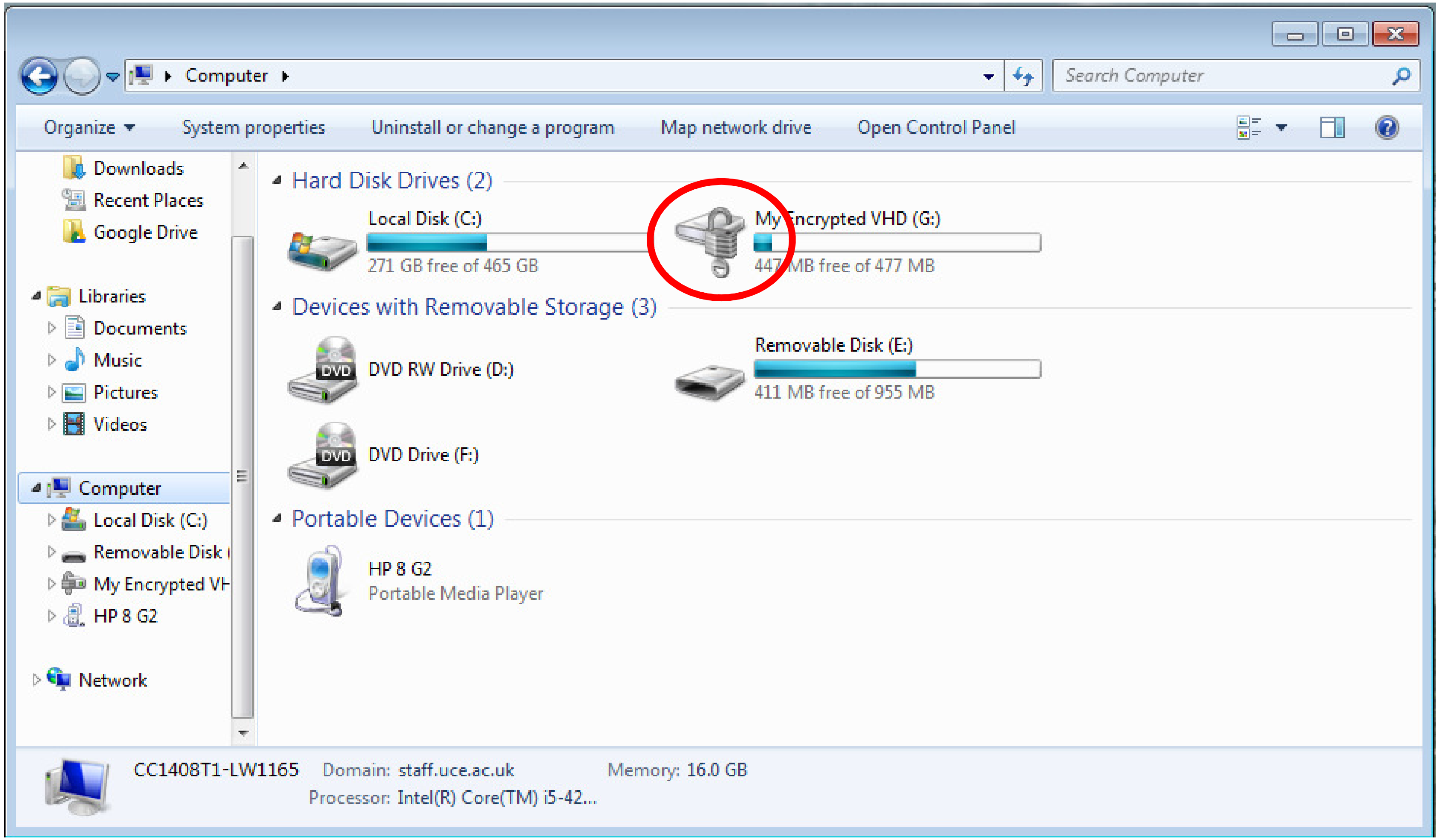
BitLocker Drive Encryption

Encrypting...

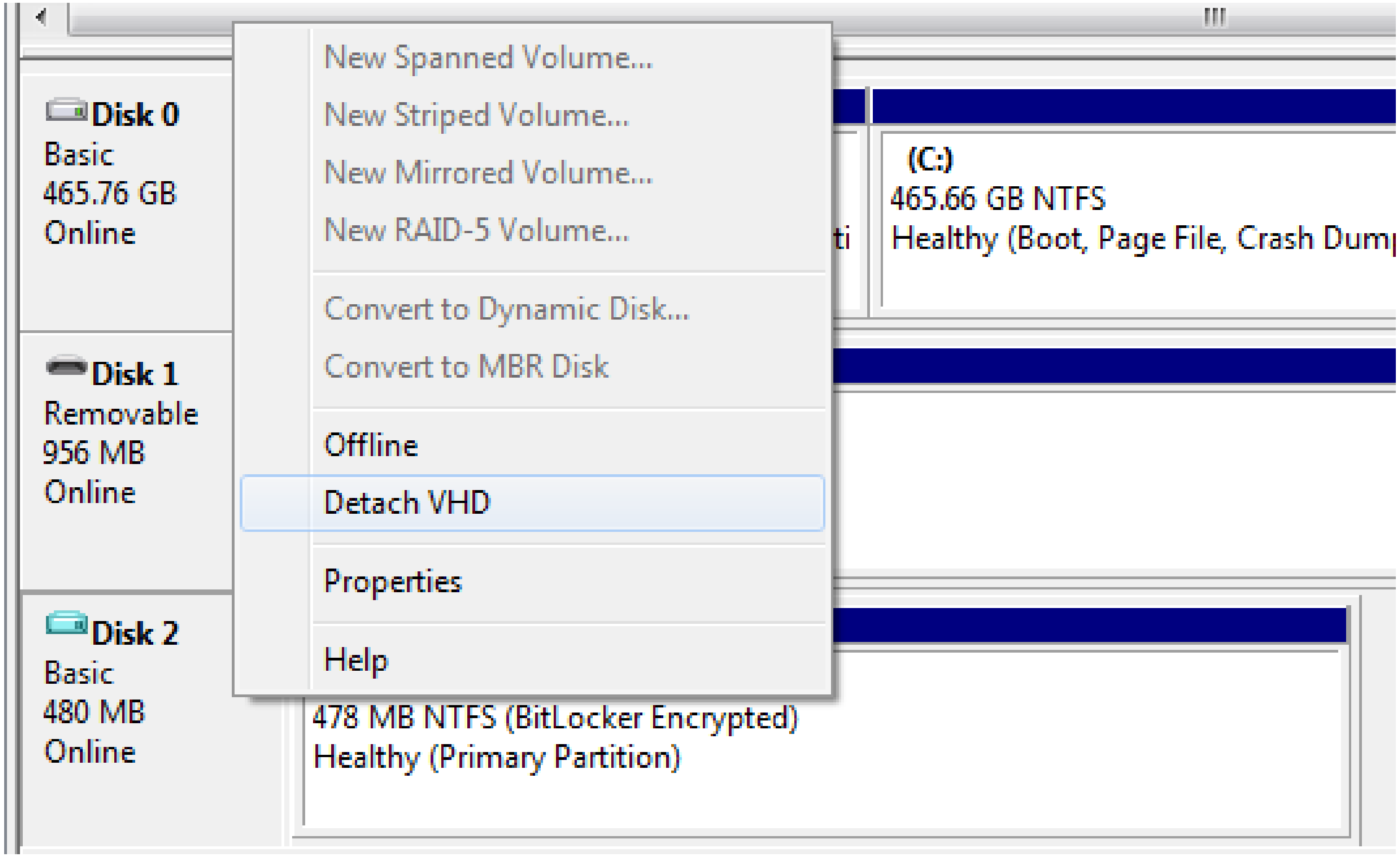
Drive G: 7.3% Completed

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

Encrypted Disk Image



Dismounting the Disk Image



Disk 0
Basic
465.76 GB
Online

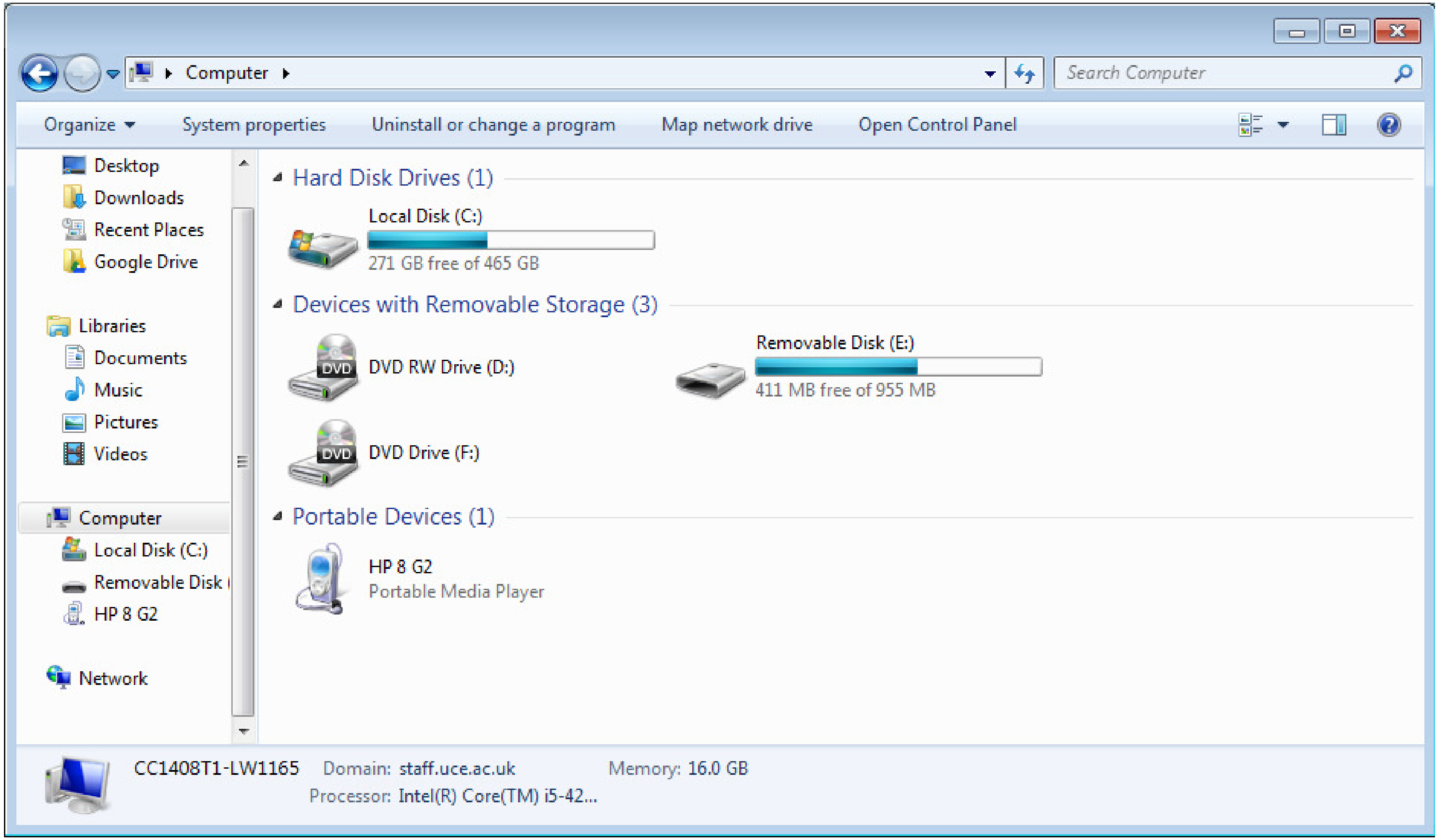
(C:)
465.66 GB NTFS
Healthy (Boot, Page File, Crash Dum

Disk 1
Removable
956 MB
Online

Disk 2
Basic
480 MB
Online

478 MB NTFS (BitLocker Encrypted)
Healthy (Primary Partition)

Dismounting the Disk Image



Hard Disk Drives (1)

Local Disk (C:)
271 GB free of 465 GB

Devices with Removable Storage (3)

DVD RW Drive (D:)

Removable Disk (E:)
411 MB free of 955 MB

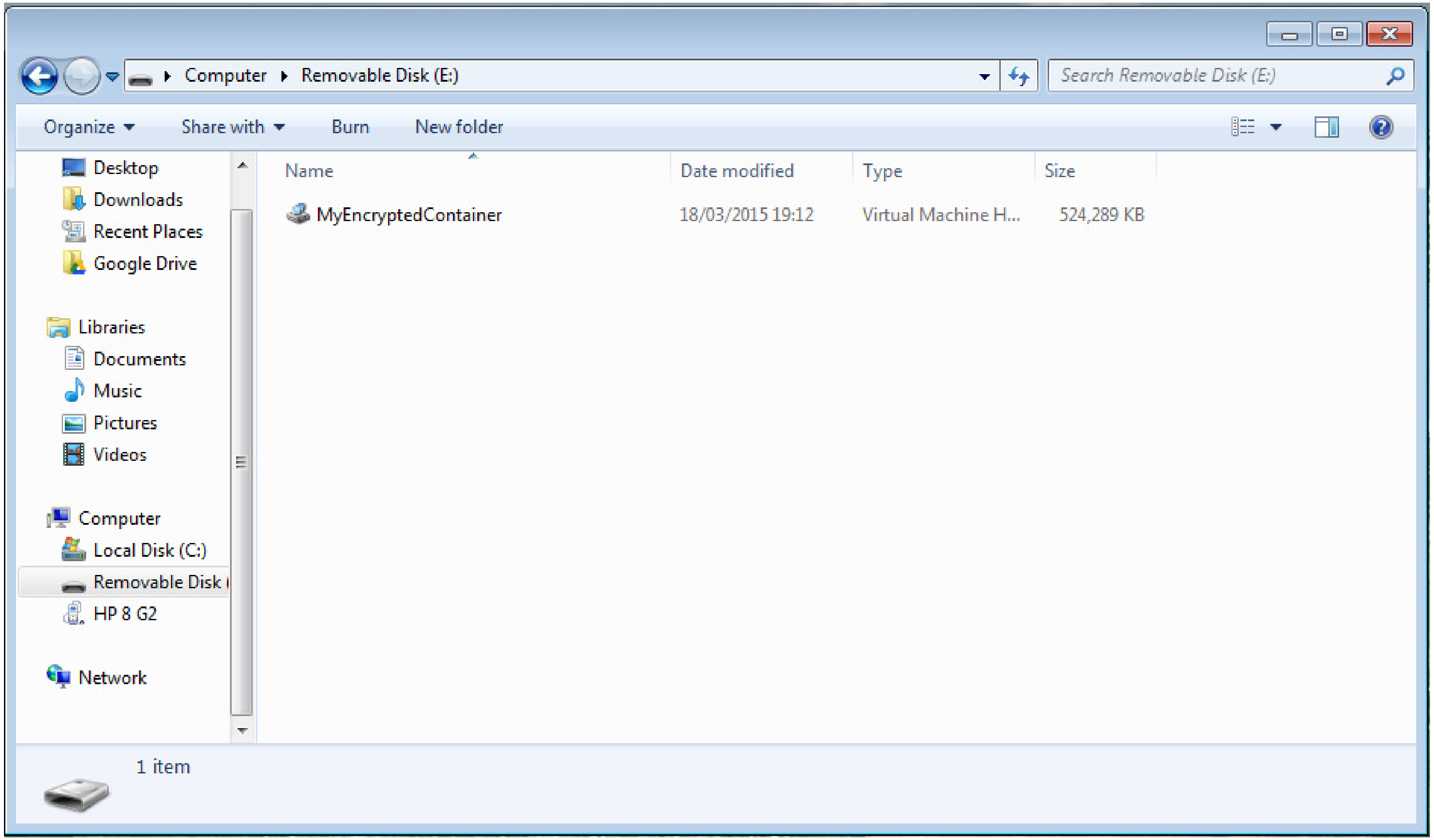
DVD Drive (F:)

Portable Devices (1)

HP 8 G2
Portable Media Player

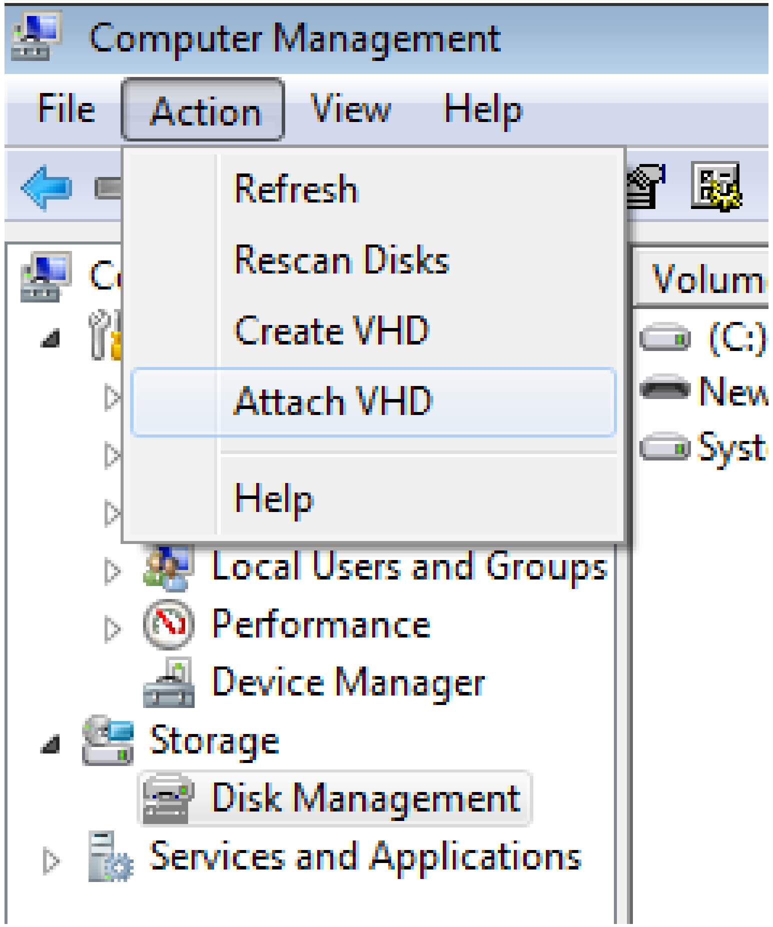
CC1408T1-LW1165 Domain: staff.uce.ac.uk Memory: 16.0 GB
Processor: Intel(R) Core(TM) i5-42...

Encrypted Container



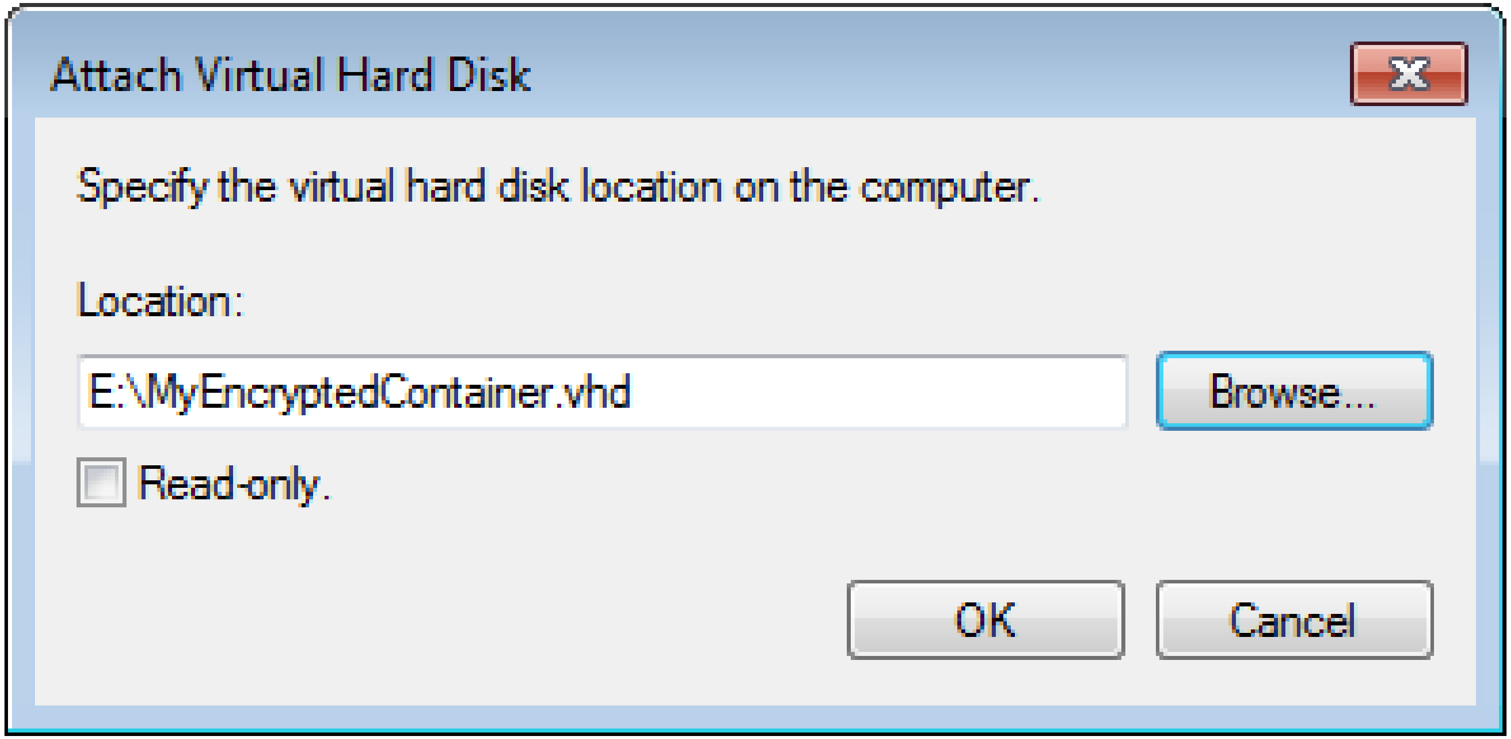
Name	Date modified	Type	Size
MyEncryptedContainer	18/03/2015 19:12	Virtual Machine H...	524,289 KB

Mounting the Disk Image



BIRMINGHAM CITY University

Mounting the Disk Image



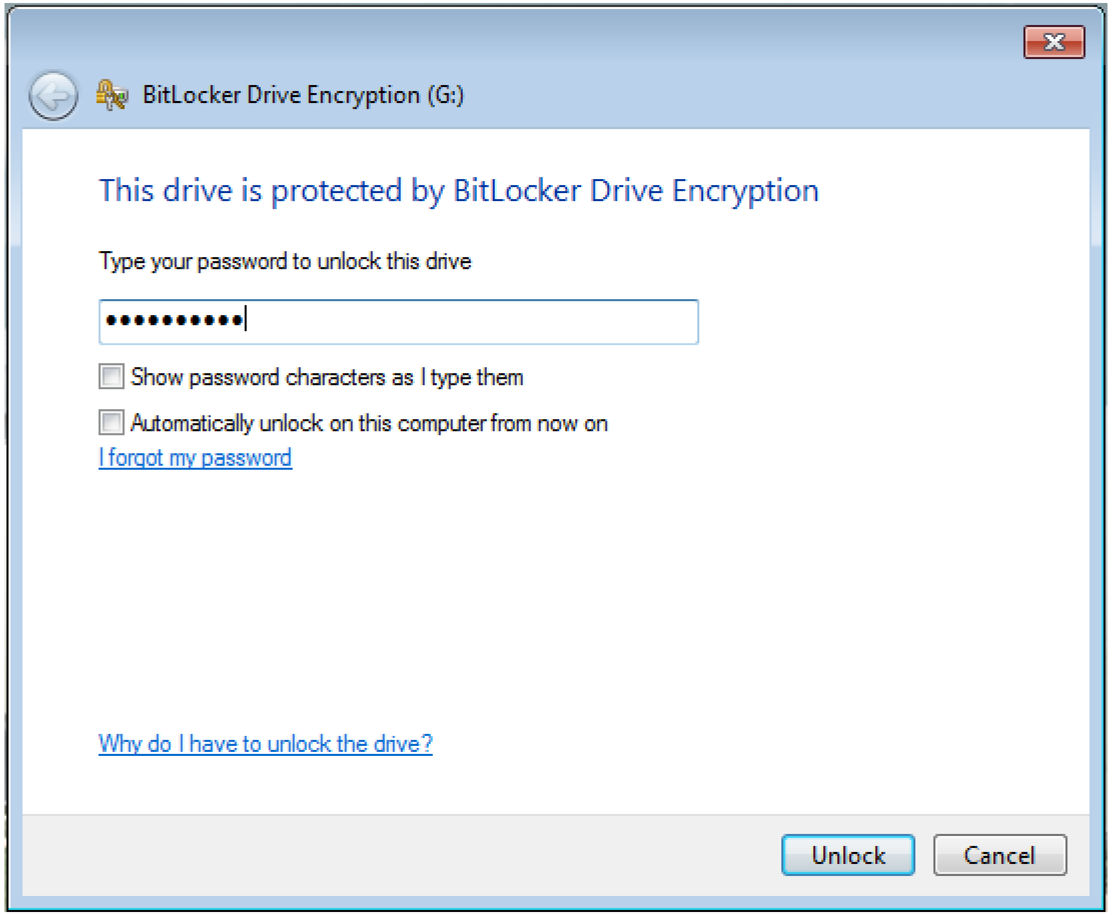
Attach Virtual Hard Disk

Specify the virtual hard disk location on the computer.

Location:

E:\MyEncryptedContainer.vhd

Mounting the Disk Image



BitLocker Drive Encryption (G:)

This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

●●●●●●●●●●●

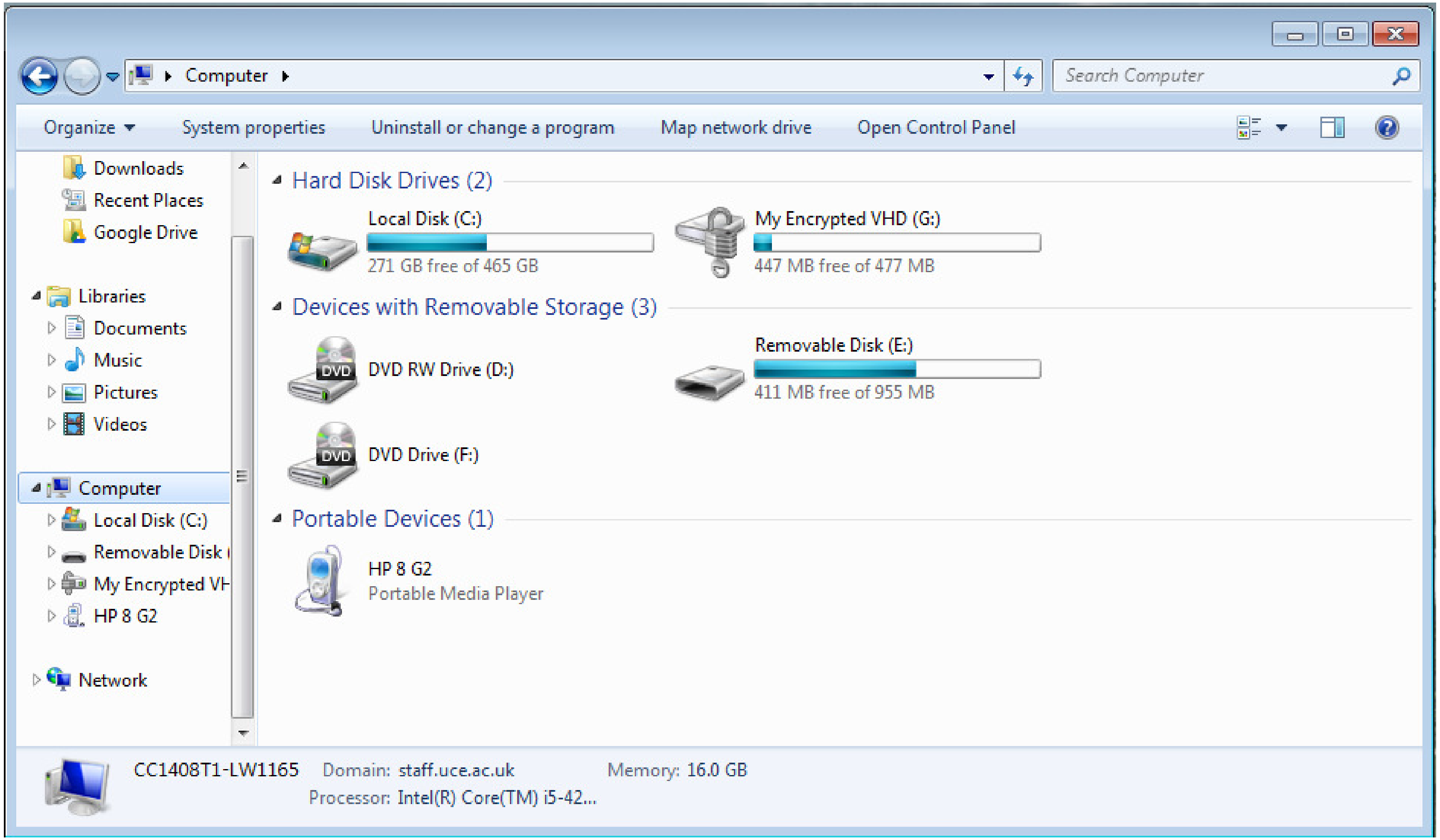
□ Show password characters as I type them

□ Automatically unlock on this computer from now on

I forgot my password

Why do I have to unlock the drive?

Mounting the Disk Image



Hard Disk Drives (2)

Local Disk (C:)
271 GB free of 465 GB

My Encrypted VHD (G:)
447 MB free of 477 MB

Devices with Removable Storage (3)

DVD RW Drive (D:)

Removable Disk (E:)
411 MB free of 955 MB

DVD Drive (F:)

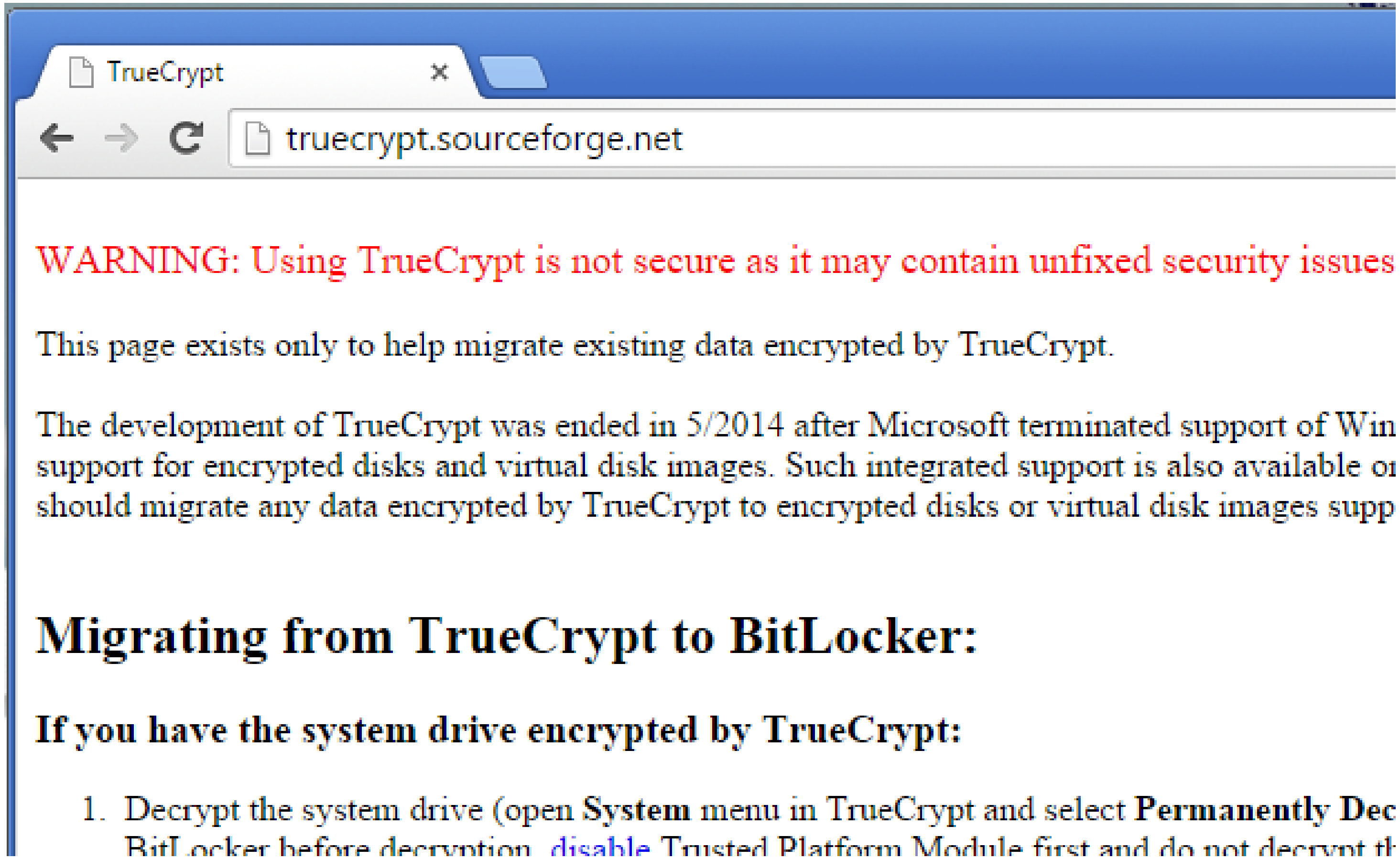
Portable Devices (1)

HP 8 G2
Portable Media Player

CC1408T1-LW1165 Domain: staff.uce.ac.uk Memory: 16.0 GB
Processor: Intel(R) Core(TM) i5-42...

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION



WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Win support for encrypted disks and virtual disk images. Such integrated support is also available o should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supp

Migrating from TrueCrypt to BitLocker:

If you have the system drive encrypted by TrueCrypt:

1. Decrypt the system drive (open **System** menu in TrueCrypt and select **Permanently Dec** BitLocker before decryption, disable Trusted Platform Module first and do not decrypt th