DATA ACQUISITION

COMP 597 – Computer Forensics

Data Acquisition

- What is a disk image?

Data Acquisition

1) Calculate the hash value for the media
2) Make a Disk image of the media
3) Calculate the hash value for the disk image

Data Acquisition

- Acquisition type
- Acquisition level
- Chunk size used
- Error handling

Acquisition Type

- Dead acquisition
- Live acquisition

Data Acquisition

1) The device under investigation is already turned off. Remove media from device then copy the media using write block protector.
2) The device is rebooted using a DVD/USB then the media is copied through the booted software.
3) Create an image of the media remotely

Acquisition Type

- Copy
- Image

Image File Format

- Raw Image
- Embedded Image
- Compressed Image

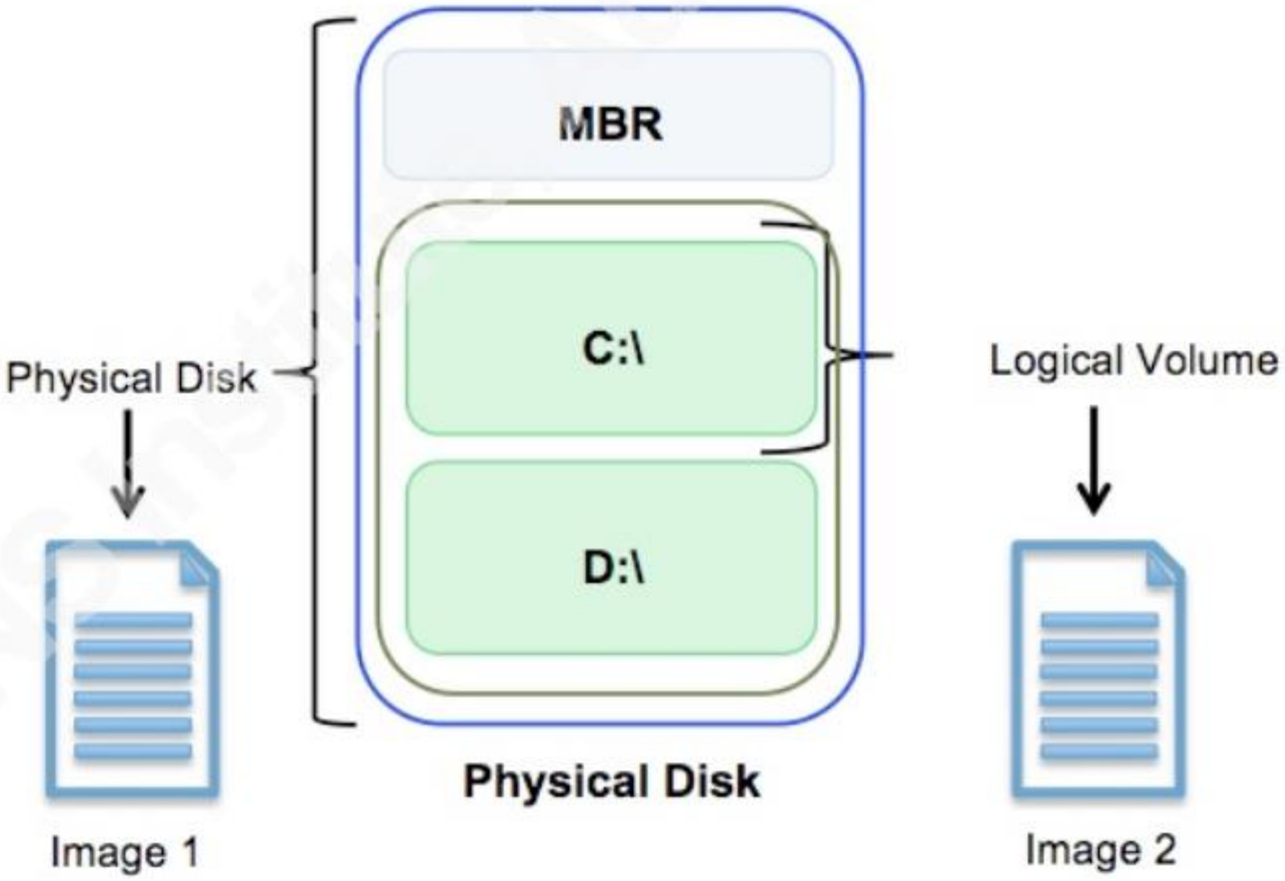
Image File Format

- E01
- dd
- AFF

Acquisition Level

- Disk
- Volume
- File

Acquisition Level



Chunk size used

- The size of chunks of data that are transferred each time

Error handling

- What happens to the acquisition process if some of the sectors are bad?

Acquisition Tools

- dd or dc3dd or dd for windows
- Helix 3
- FTK Imager
- EnCase Forensic Imager
- DFF

dd

- Command line-based
- Byte wise copy

dd

Parameters:

- if
- of
- bs
- count
- skip
- conv

dd

- dd --list

dd

```
dd if=file1.dat of=file2.dat bs=512
2+0 records in
2+0 records out
```

dd

```
dd if=/dev/hda of=/mnt/hda.dd bs=2k
dd if=/dev/hda of=/dev/hdd bs=2k
dd if=/dev/hdb bs=512 skip=15000 count=1
```

dd - Error Handling

- dd if=/dev/hda of=hda.dd bs=2k conv=noerror,sync

HPA

- diskstat /dev/hdb

Forensic Analysis

Forensic analysis can either be done:

- on the image directly
- by mounting the image

Mount Type

- Block Device/Read Only
- Block Device/Writable
- File System/Read Only

Mounting an Image as VM

Mounting an Image as VM

1. Virtualization Software
2. Forensic image should be loaded as a disk
3. Writing commands should be cached

Mounting an Image as VM

- Mount the image
- Create a virtual machine disk
  - cd c:\program files\oracle\virtualbox

  - vboxmanage internalcommands createrawvmdk -filename c:\test.vmdk -rawdisk \\.\physicaldrive2
- Start a new VM

USB Write Block

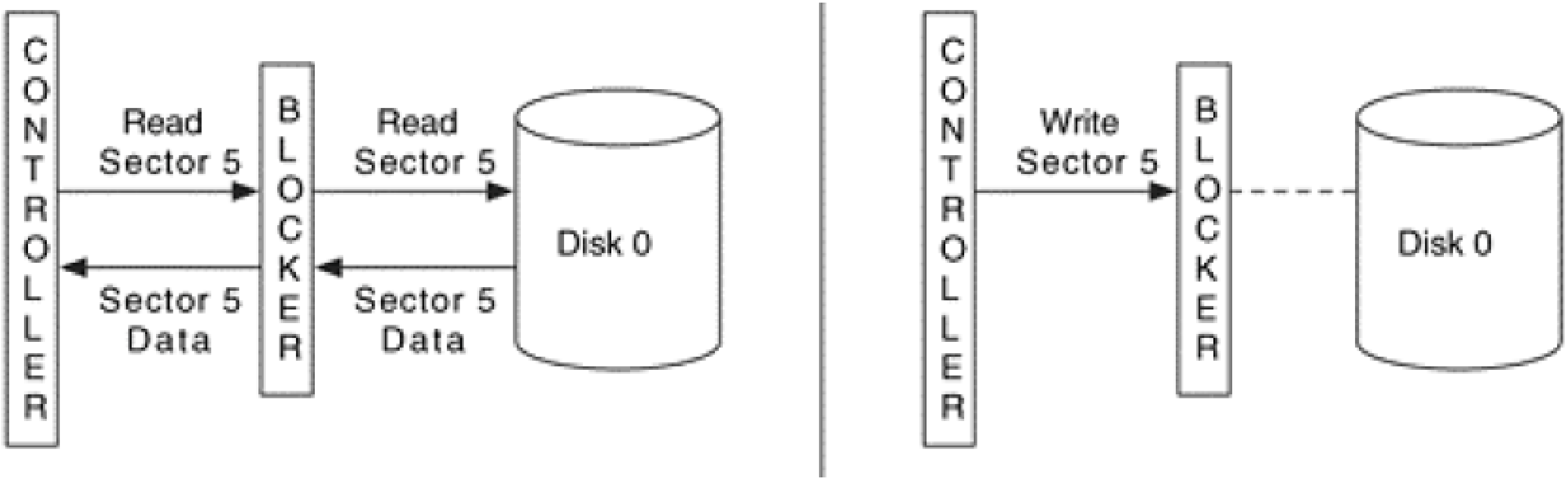
Data Acquisition

- Why is it important o have write blocking for USB drives?

Data Acquisition

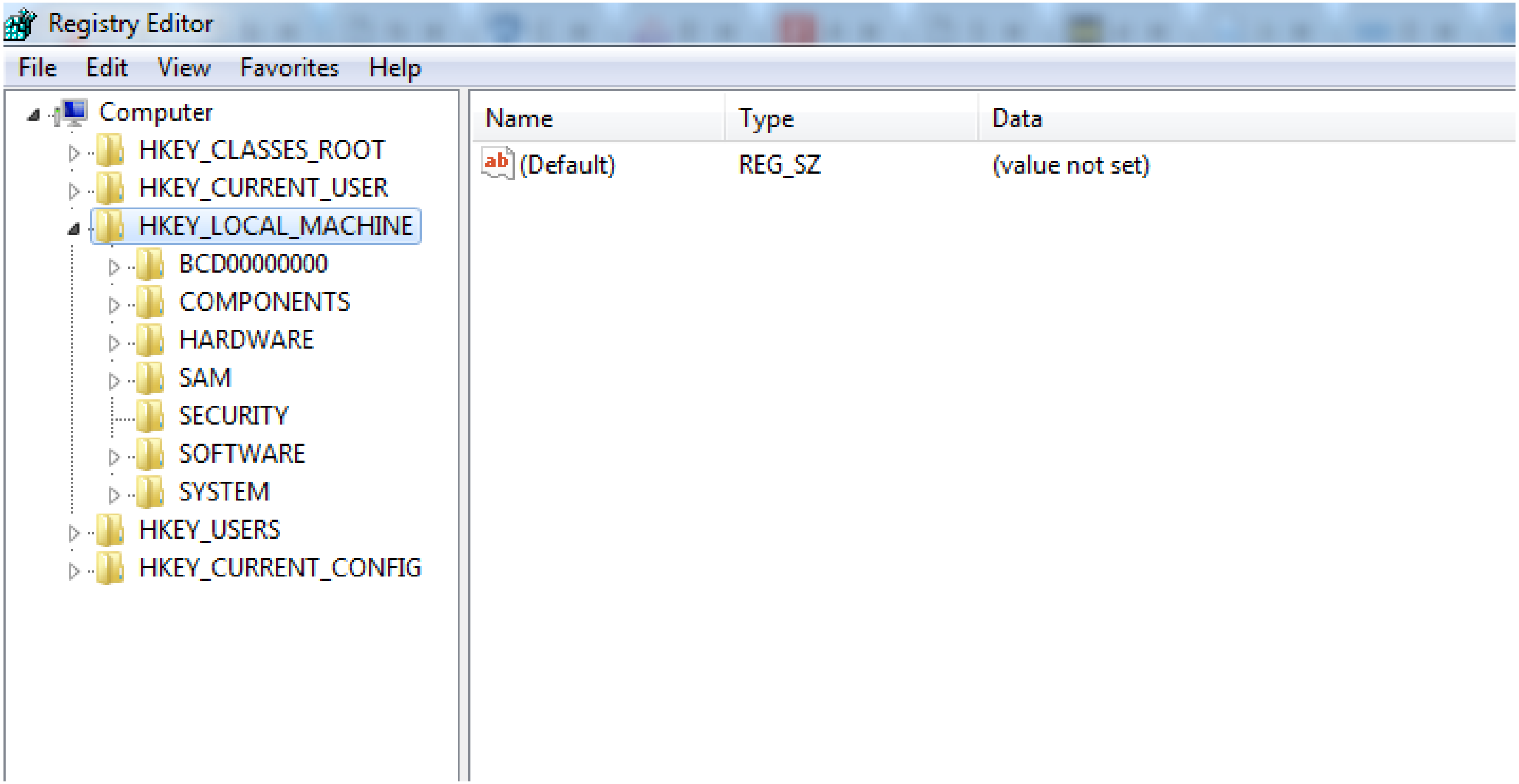
- Hardware writer blocker
- Software write blocker

Hardware writer blocker



From: File System Forensic Analysis, 2nd edition, Brian Carrier

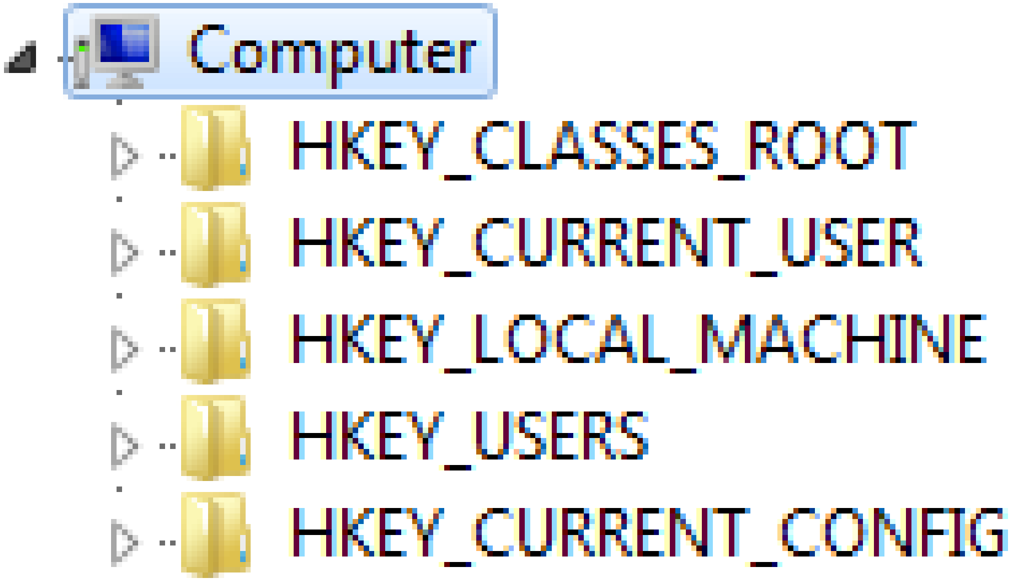
Windows Registry



Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
  - BCD00000000
  - COMPONENTS
  - HARDWARE
  - SAM
  - SECURITY
  - SOFTWARE
  - SYSTEM
- HKEY_USERS
- HKEY_CURRENT_CONFIG

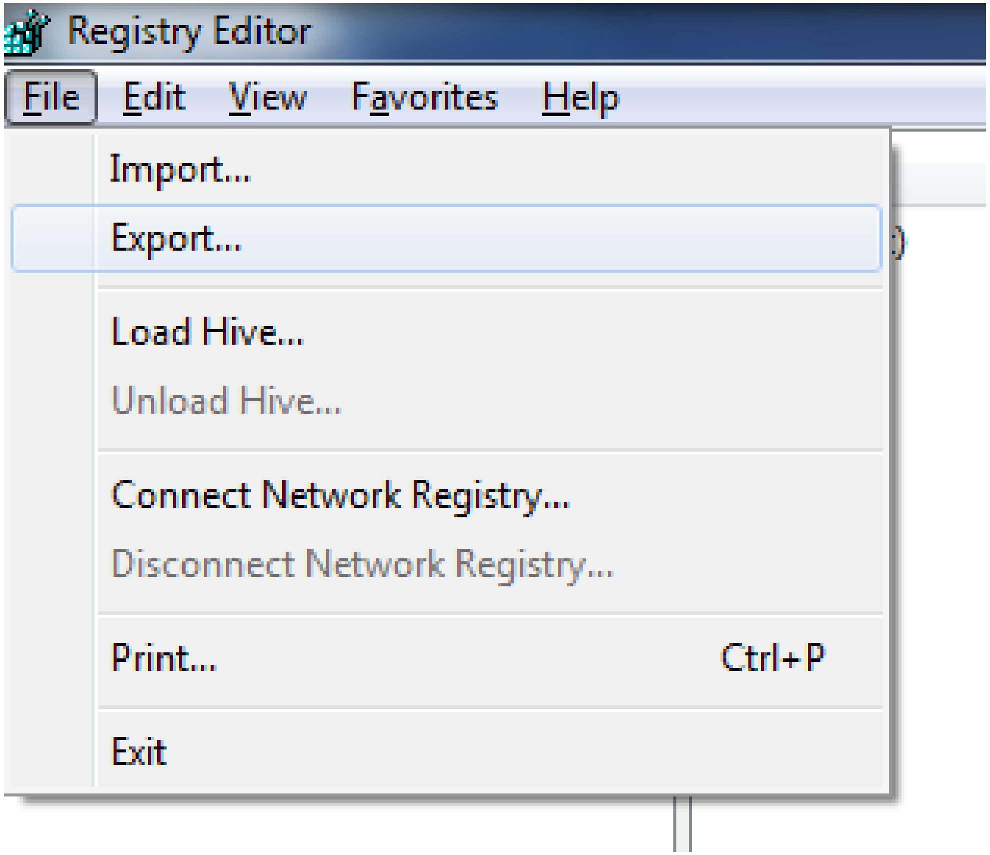
Name	Type	Data
(Default)	REG_SZ	(value not set)

Windows Registry

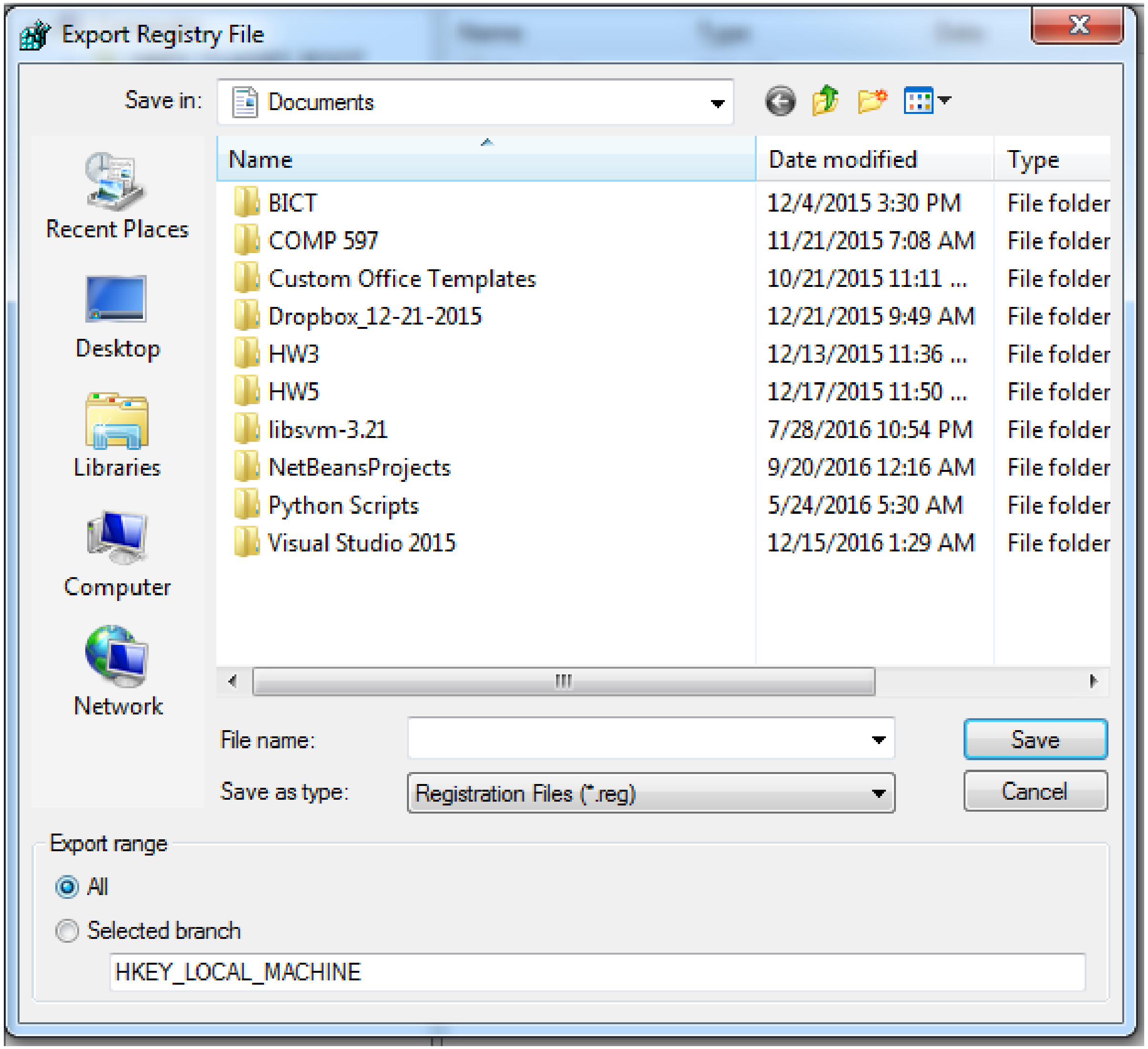


- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG

Windows Registry



Windows Registry



Export Registry File

Save in: Documents

Name	Date modified	Type
BICT	12/4/2015 3:30 PM	File folder
COMP 597	11/21/2015 7:08 AM	File folder
Custom Office Templates	10/21/2015 11:11 ...	File folder
Dropbox_12-21-2015	12/21/2015 9:49 AM	File folder
HW3	12/13/2015 11:36 ...	File folder
HW5	12/17/2015 11:50 ...	File folder
libsvm-3.21	7/28/2016 10:54 PM	File folder
NetBeansProjects	9/20/2016 12:16 AM	File folder
Python Scripts	5/24/2016 5:30 AM	File folder
Visual Studio 2015	12/15/2016 1:29 AM	File folder

File name:

Save as type: Registration Files (*.reg)

Export range

● All

○ Selected branch

HKEY_LOCAL_MACHINE

Write Protect

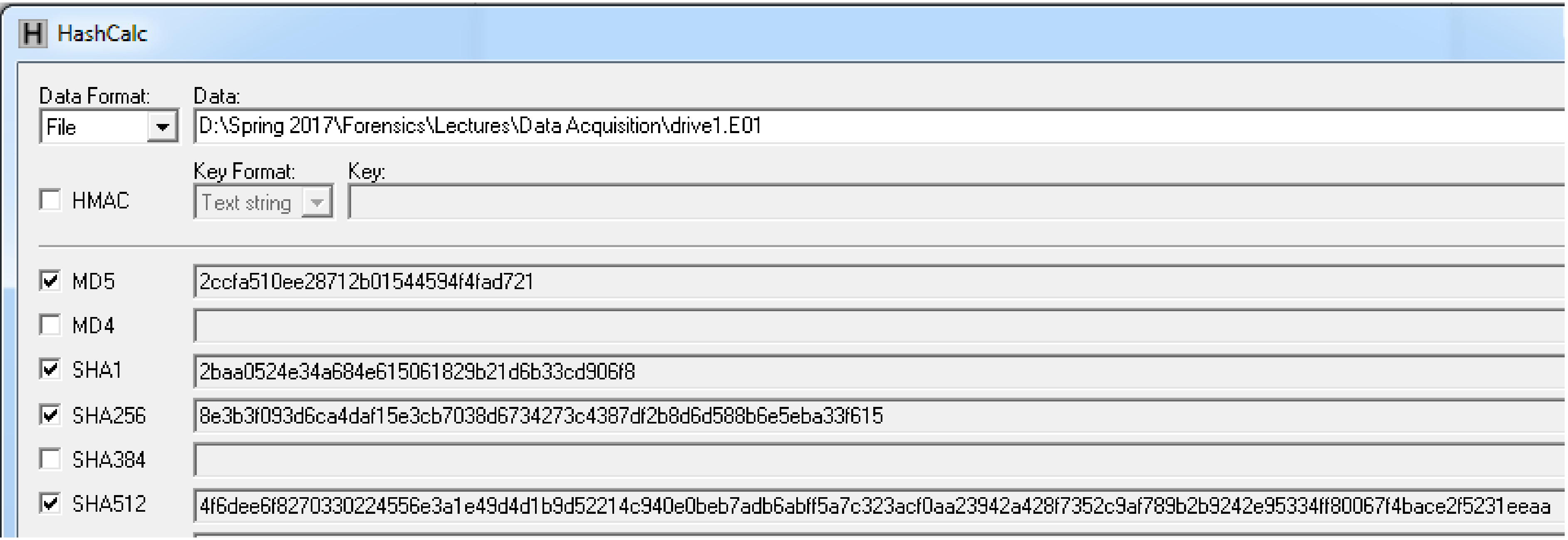
1) Go to *HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control*
2) Add a new key called *StorageDevicePolicies*
3) Add a new value *WriteProtect* with value 1

Validation of Data Images

Hashing Evidence Files

- We are going to:
  - Calculate the hash value of the image file
  - Calculate the hash value of the contents of the image file

HashCalc



Data Format: File

Data: D:\Spring 2017\Forensics\Lectures\Data Acquisition\drive1.E01

□ HMAC

Key Format: Text string

Key:

☑ MD5 2ccfa510ee28712b01544594f4fad721

□ MD4

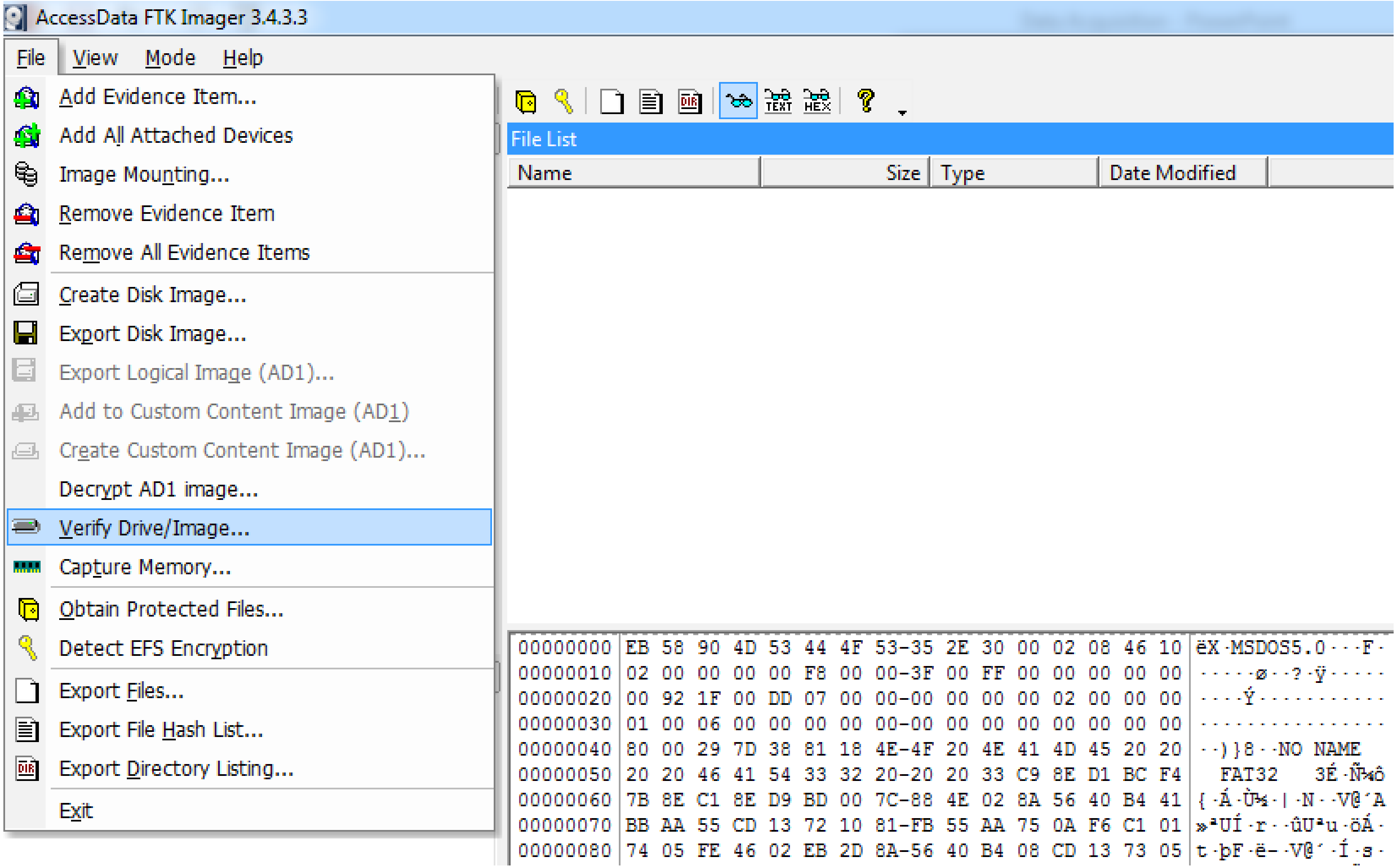
☑ SHA1 2baa0524e34a684e615061829b21d6b33cd906f8

☑ SHA256 8e3b3f093d6ca4daf15e3cb7038d6734273c4387df2b8d6d588b6e5eba33f615

□ SHA384

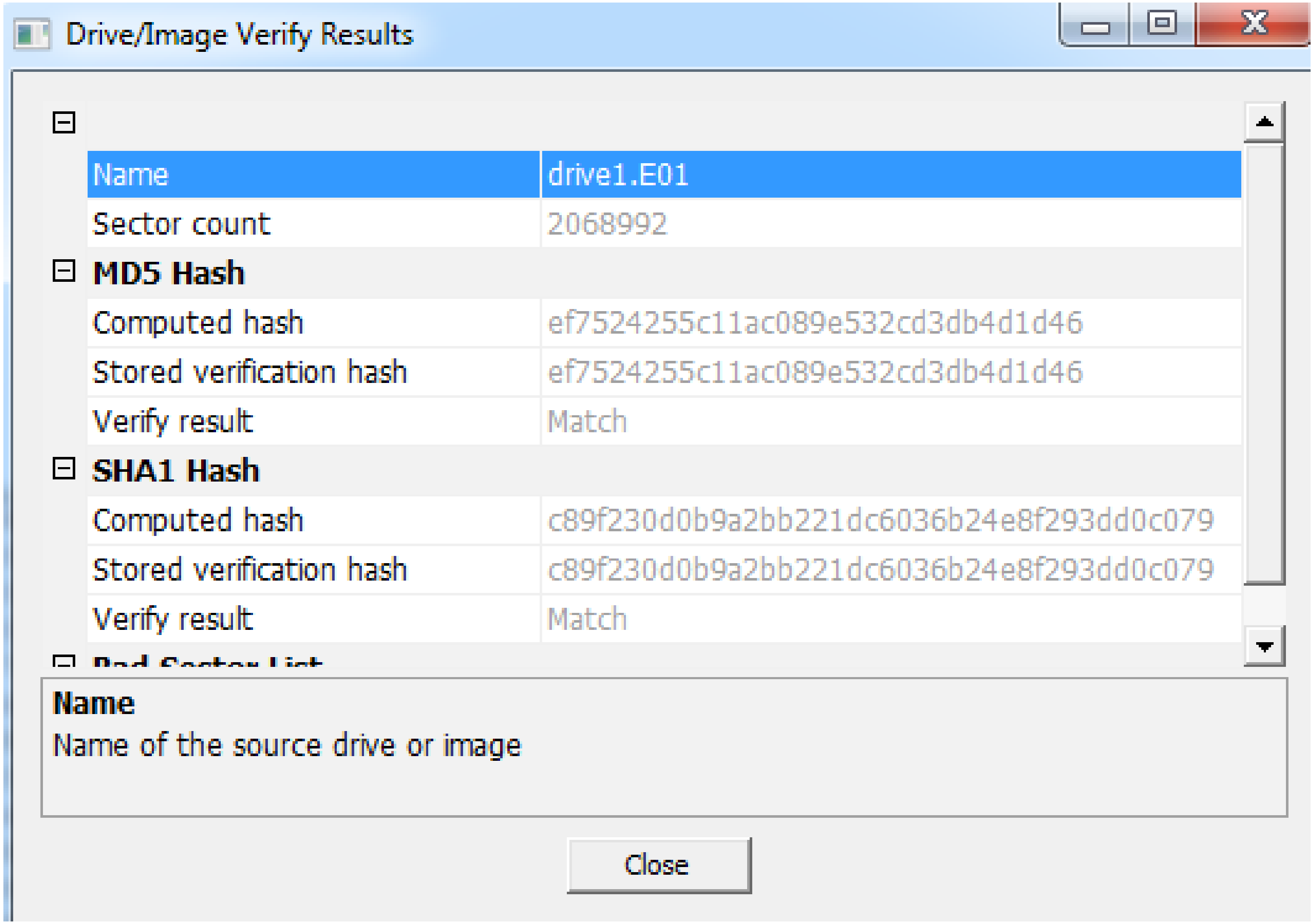
☑ SHA512 4f6dee6f8270330224556e3a1e49d4d1b9d52214c940e0beb7adb6abff5a7c323acf0aa23942a428f7352c9af789b2b9242e95334ff80067f4bace2f5231eeaa

FTK Imager



```
00000000 EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 08 46 10 ëX·MSDOS5.0···F·
00000010 02 00 00 00 00 F8 00 00-3F 00 FF 00 00 00 00 00 ·····ø··?·ÿ·····
00000020 00 92 1F 00 DD 07 00 00-00 00 00 00 02 00 00 00 ····Ý···········
00000030 01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000040 80 00 29 7D 38 81 18 4E-4F 20 4E 41 4D 45 20 20 ··)}8··NO NAME  
00000050 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4   FAT32   3É·Ñ¼ô
00000060 7B 8E C1 8E D9 BD 00 7C-88 4E 02 8A 56 40 B4 41 {·Á·Ù½·|·N··V@´A
00000070 BB AA 55 CD 13 72 10 81-FB 55 AA 75 0A F6 C1 01 »ªUÍ·r··ûUªu·öÁ·
00000080 74 05 FE 46 02 EB 2D 8A-56 40 B4 08 CD 13 73 05 t·þF·ë-·V@´·Í·s·
```

FTK Imager



Drive/Image Verify Results

Name	drive1.E01
Sector count	2068992
MD5 Hash	
Computed hash	ef7524255c11ac089e532cd3db4d1d46
Stored verification hash	ef7524255c11ac089e532cd3db4d1d46
Verify result	Match
SHA1 Hash	
Computed hash	c89f230d0b9a2bb221dc6036b24e8f293dd0c079
Stored verification hash	c89f230d0b9a2bb221dc6036b24e8f293dd0c079
Verify result	Match
Bad Sector List	

Name

Name of the source drive or image

References

- File System Forensic Analysis, 2nd edition, Brian Carrier, 2005.