DIGITAL FORENSICS LAB SERIES

Lab 3: Hashing Data Sets

Objective: Evidence Acquisition, Preparation and Preservation

Document Version: 2015-09-28

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

This lab includes the following tasks:

1. Imaging and Hashing a Disk and Verifying the Hashes of the Image
2. Using BackTrack to Hash Images, Disks, and Partitions
3. Using HashCalc to Verify Hashes

Objective: Digital Forensics Fundamentals

Performing this lab will provide the student with a hands-on lab experience meeting the Digital Forensics Fundamentals Objective:

The candidate will demonstrate an understanding of forensic methodology, key forensics concepts, and identifying types of evidence on current Windows operating systems.

A forensic examination is not performed on a suspect's actual drive. A copy, or image, of the drive is made and then the examination is performed on the copy. A hash, like MD5 or SHA1 can be used to prove that the copy is forensically equivalent to the actual disk.

EnCase Imager – Encase Imager is a GUI Program that will allow a user to create a disk image from within Windows. You can run into complications imaging a disk while in Windows because certain files are locked by the OS. EnCase Imager is a free product.

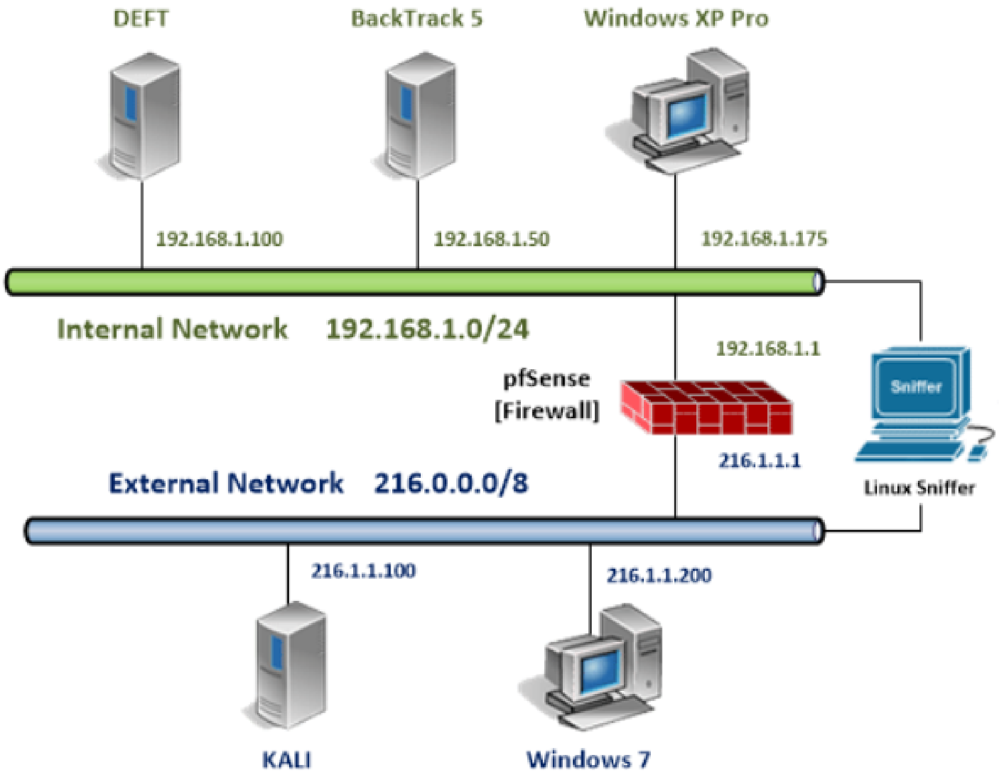
HashCalc – A free program from http://www.slavasoft.com/hashcalc/ that allows you to calculate the MD5, SHA-256, SHA-384, SHA-512, and other hash values of data sets.

MD5 – Message Digest 5 is a 128 bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is 'equivalent' to the original. Other hashes, like SHA-1, which is 160 bits, are more accurate than the 128 bit MD5.

SHA1 – Secure Hash Algorithm is a 160 bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is 'equivalent' to the original. There are also 256, 384, and 512 bit versions of SHA that are more accurate.

BackTrack– BackTrack is a free Ubuntu Linux-based Live DVD. BackTrack, from Offensive-Security, is used for forensics and penetration testing. It is available for download free at the following link: http://www.backtrack-linux.org/downloads/.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

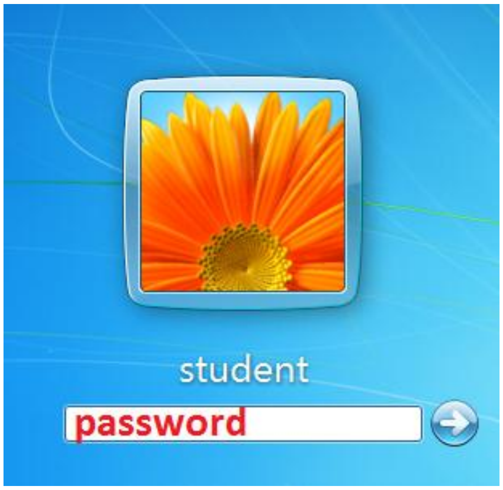
Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Windows 7 External Machine	216.1.1.200	student	password

1 Imaging and Hashing a Disk and Verifying the Hashes of the Image

Disks are imaged, or copied, so that an examiner can work on a copy of the disk as opposed to analyzing the actual drive. A disk can be imaged and hashed from within Windows using a Graphical User Interface (GUI) based tool like EnCase Imager. EnCase Imager is a free product that is made by Guidance Software. After a disk is imaged with EnCase Imager, you will receive an acquisition and verification hash. When the image is loaded into a case, the acquisition hash should match the verification hash.

1.1 Using EnCase Imager

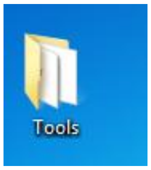
1. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password,** and press **Enter** to log in.



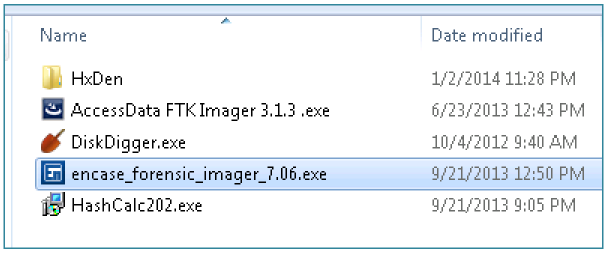
student

password

1. Double-click on the Tools folder on the desktop.

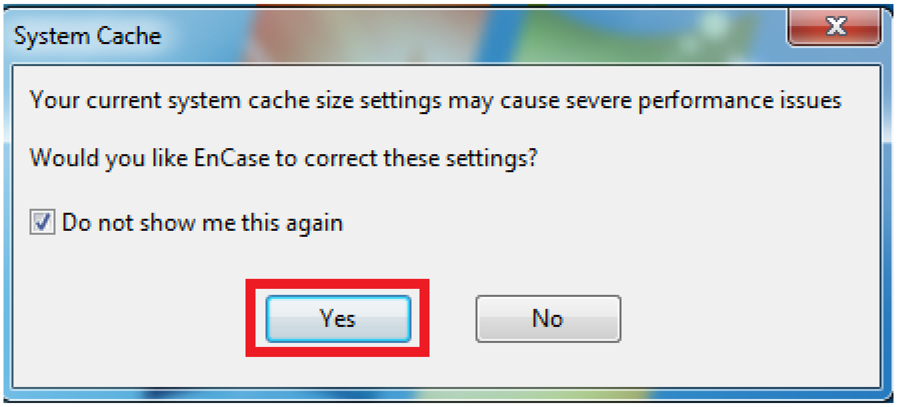


2. Double-click on **encase_forensic_imager_7.06.exe** to launch the program.



Name	Date modified
HxDen	1/2/2014 11:28 PM
AccessData FTK Imager 3.1.3 .exe	6/23/2013 12:43 PM
DiskDigger.exe	10/4/2012 9:40 AM
encase_forensic_imager_7.06.exe	9/21/2013 12:50 PM
HashCalc202.exe	9/21/2013 9:05 PM

3. Click **Yes** when you are asked if you want EnCase to correct the settings.



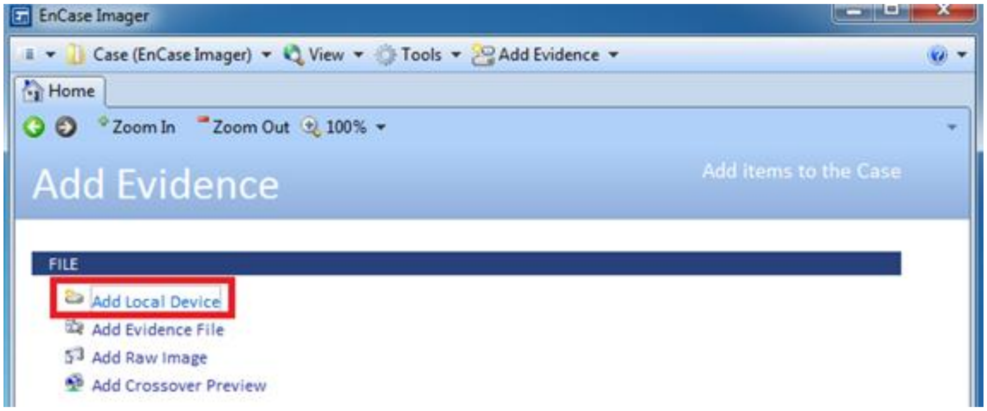
System Cache

Your current system cache size settings may cause severe performance issues

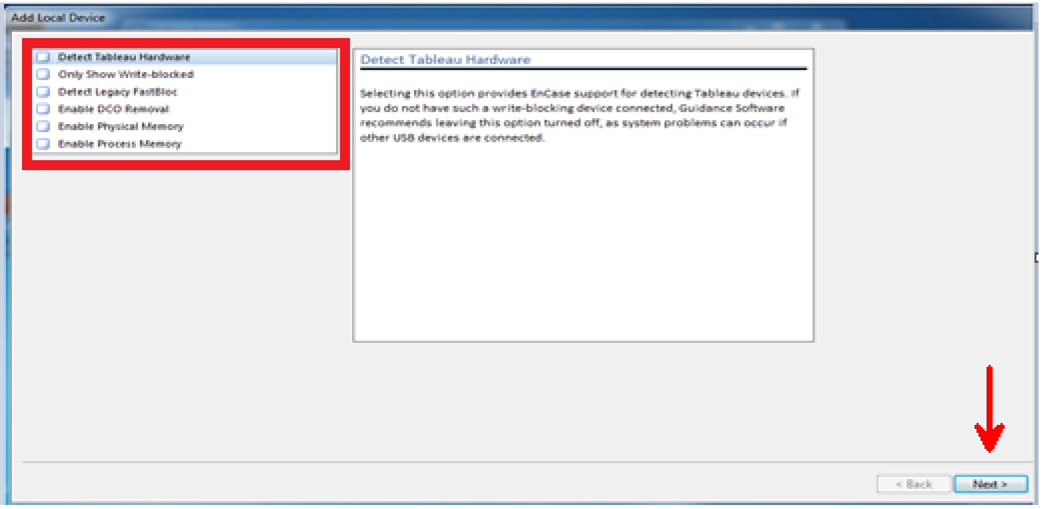
Would you like EnCase to correct these settings?

☑ Do not show me this again

4. At the Encase Imager Add Evidence screen, click **Add Local Device**.



5. At the Add Local Device screen, **uncheck all of the boxes**. Click **Next**.



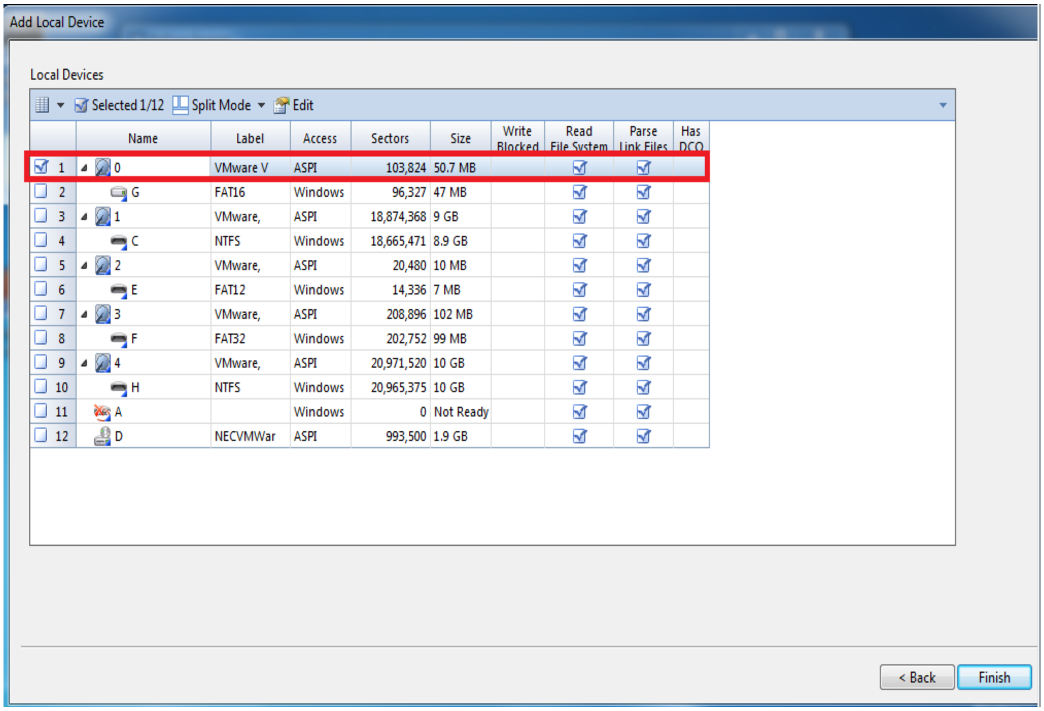
Add Local Device

□ Detect Tableau Hardware
□ Only Show Write-blocked
□ Detect Legacy FastBloc
□ Enable DCO Removal
□ Enable Physical Memory
□ Enable Process Memory

Detect Tableau Hardware

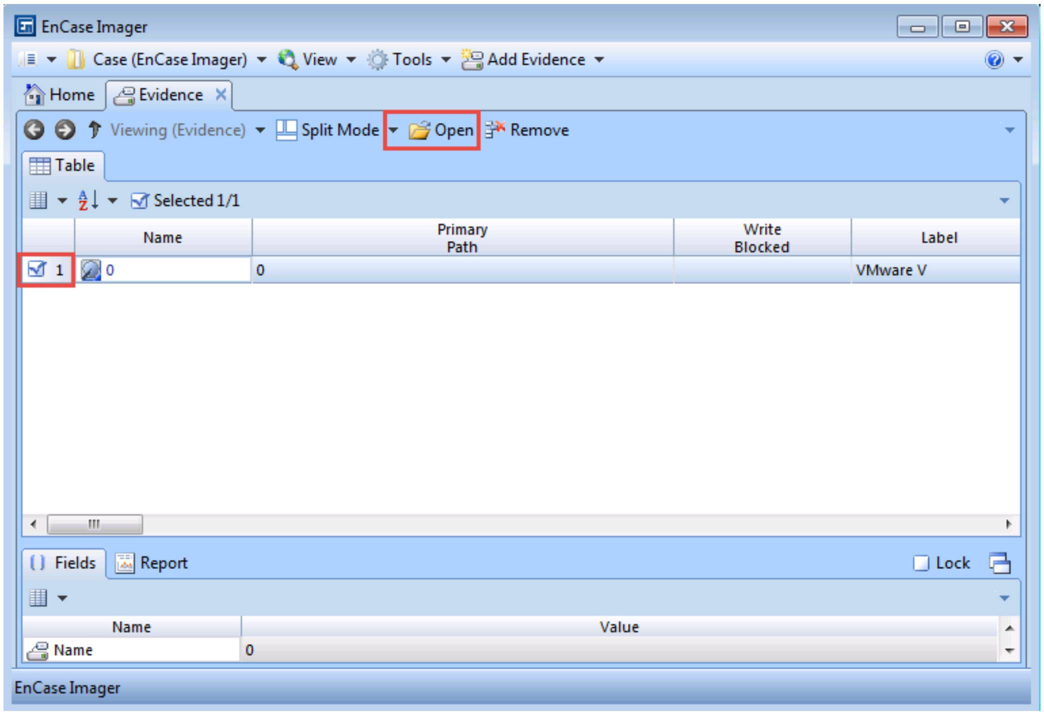
Selecting this option provides EnCase support for detecting Tableau devices. If you do not have such a write-blocking device connected, Guidance Software recommends leaving this option turned off, as system problems can occur if other USB devices are connected.

6. Click the first box to select disk 0, with a size of 50.7 MB. Click **Finish**.



		Name	Label	Access	Sectors	Size	Write Blocked	Read File System	Parse Link Files	Has DCO
☑	1	0	VMware V	ASPI	103,824	50.7 MB		☑	☑	
□	2	G	FAT16	Windows	96,327	47 MB		☑	☑	
□	3	1	VMware,	ASPI	18,874,368	9 GB		☑	☑	
□	4	C	NTFS	Windows	18,665,471	8.9 GB		☑	☑	
□	5	2	VMware,	ASPI	20,480	10 MB		☑	☑	
□	6	E	FAT12	Windows	14,336	7 MB		☑	☑	
□	7	3	VMware,	ASPI	208,896	102 MB		☑	☑	
□	8	F	FAT32	Windows	202,752	99 MB		☑	☑	
□	9	4	VMware,	ASPI	20,971,520	10 GB		☑	☑	
□	10	H	NTFS	Windows	20,965,375	10 GB		☑	☑	
□	11	A		Windows	0	Not Ready		☑	☑	
□	12	D	NECVMWar	ASPI	993,500	1.9 GB		☑	☑	

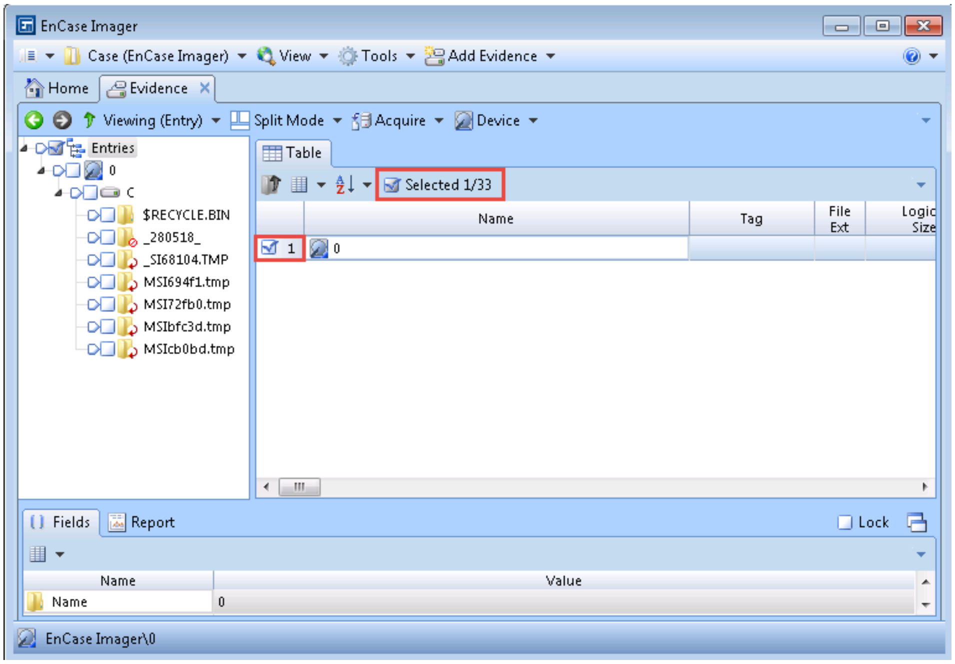
7. Verify that the Disk is selected with check mark. Click the **Open** button in the middle of the screen.



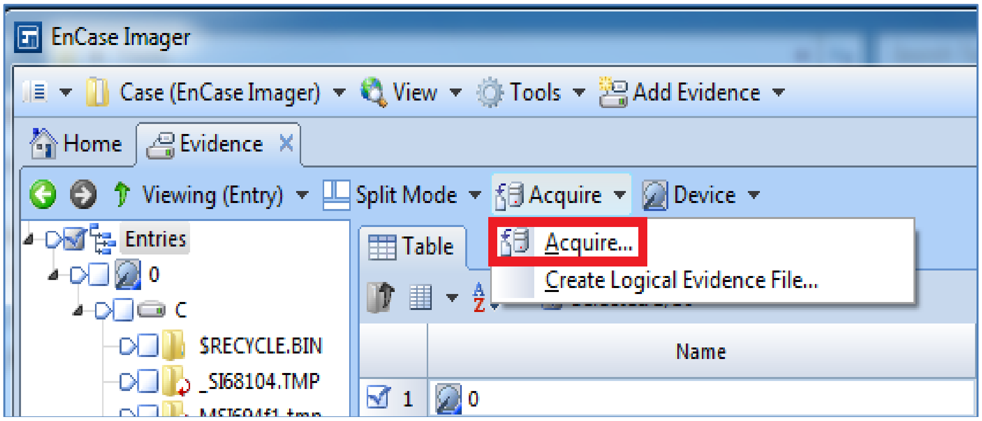
		Name	Primary Path	Write Blocked	Label
☑	1	0	0		VMware V

Name	Value
Name	0

8. Check the disk in the table pane. It should state that **0/33** or **1/33** items is selected.

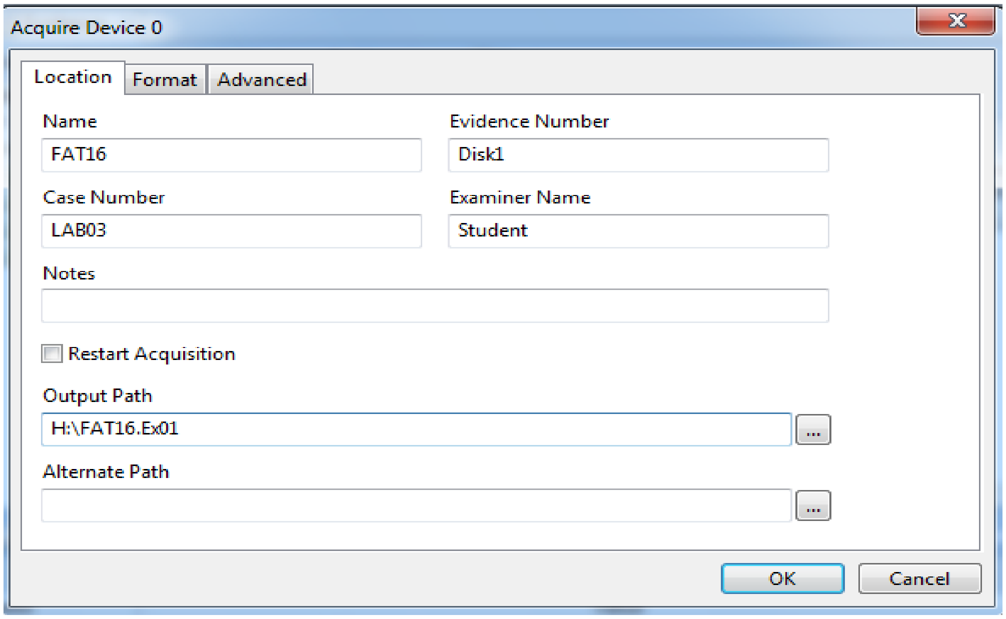


9. Click the arrow to the right of Acquire and select **Acquire** from the menu.



10. Input the following information in the fields of the **Acquire Device 0** screen.

Field	Entry
Name	FAT16
Evidence Number	Disk1
Case Number	LAB03
Examiner Name	Student
Output Path	H:\FAT16.Ex01



Name: FAT16

Evidence Number: Disk1

Case Number: LAB03

Examiner Name: Student

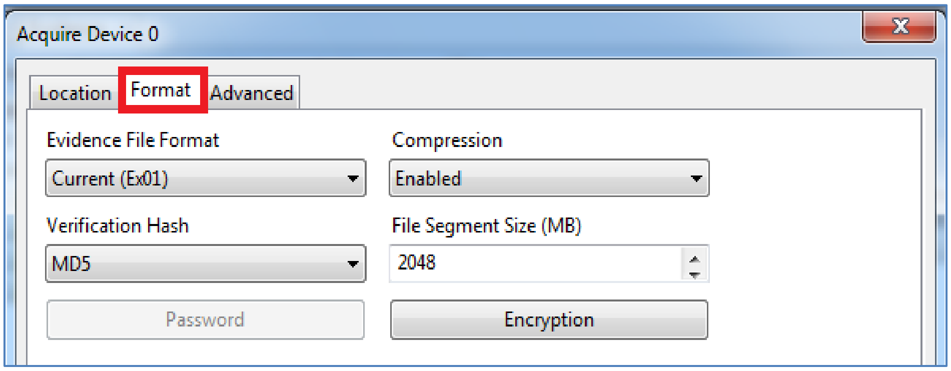
Notes:

□ Restart Acquisition

Output Path: H:\FAT16.Ex01

Alternate Path:

11. Click the **Format** tab of the Acquire Device 0 screen,



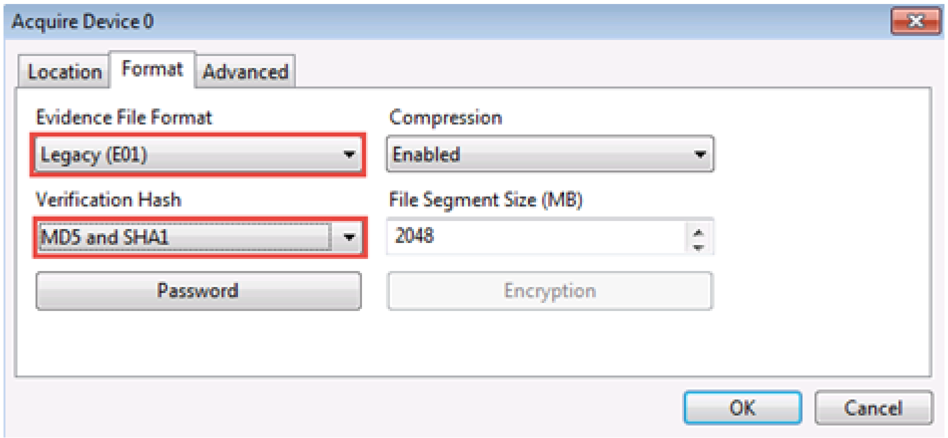
Evidence File Format: Current (Ex01)

Compression: Enabled

Verification Hash: MD5

File Segment Size (MB): 2048

12. In the Dropdown boxes, change the Evidence File Format from Current (Ex01) to Legacy (E01). In the Verification Hash dropdown box, select the MD5 and SHA1 hashes.



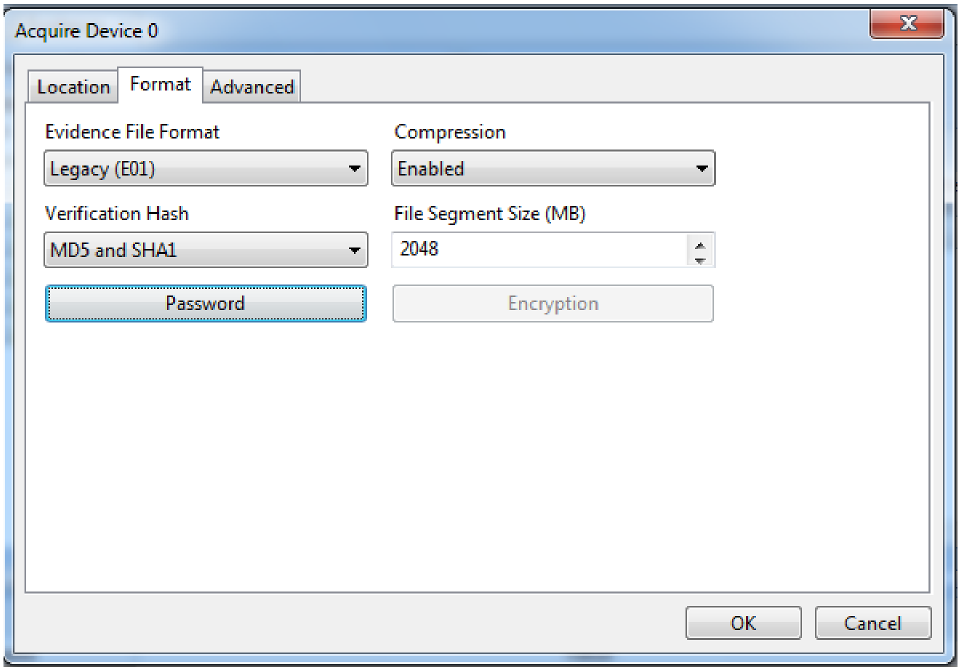
Evidence File Format: Legacy (E01)

Compression: Enabled

Verification Hash: MD5 and SHA1

File Segment Size (MB): 2048

13. Notice that when the image type is changed (Evidence File Format), the password box becomes available. This will allow the investigator to password protect the disk image being created. Click **OK**.


Acquire Device 0

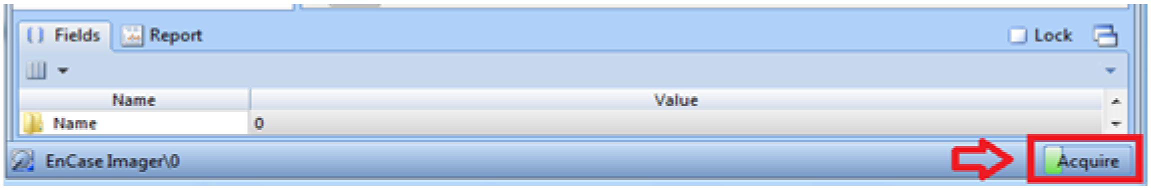
Evidence File Format: Legacy (E01)

Compression: Enabled

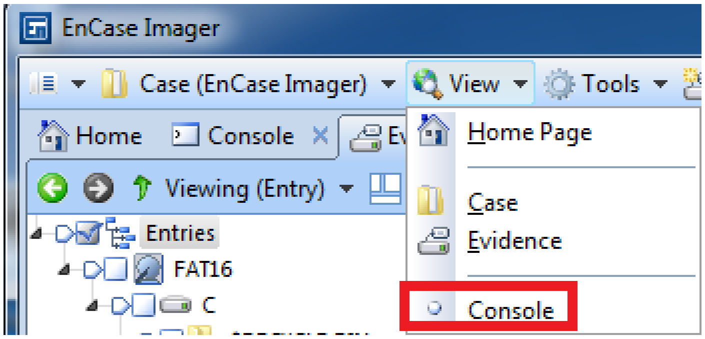
Verification Hash: MD5 and SHA1

File Segment Size (MB): 2048

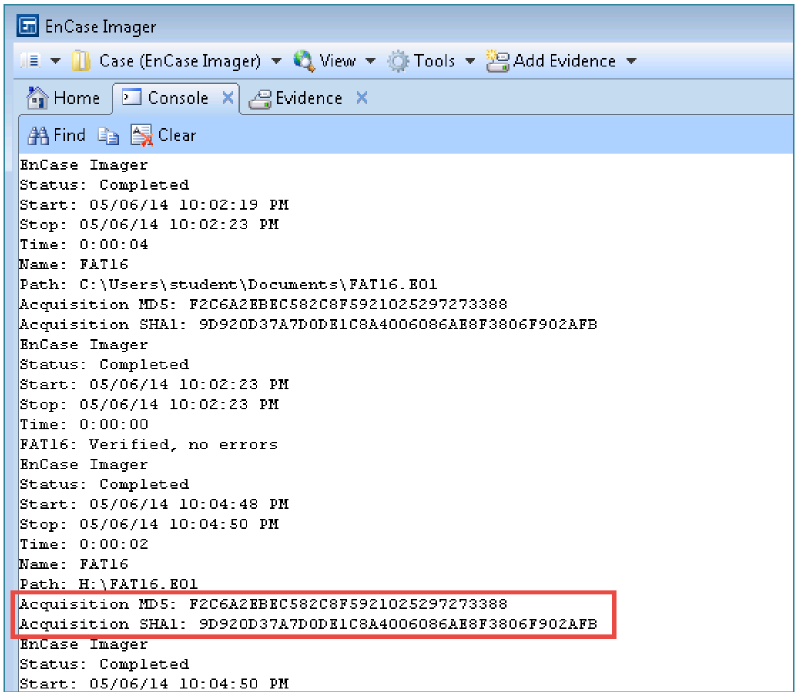
14. A box in the lower-right corner will appear, indicating acquiring, then verifying. This happens quickly.


Name	Value
Name	0

15. From the View menu, select **Console** to view acquisition information.

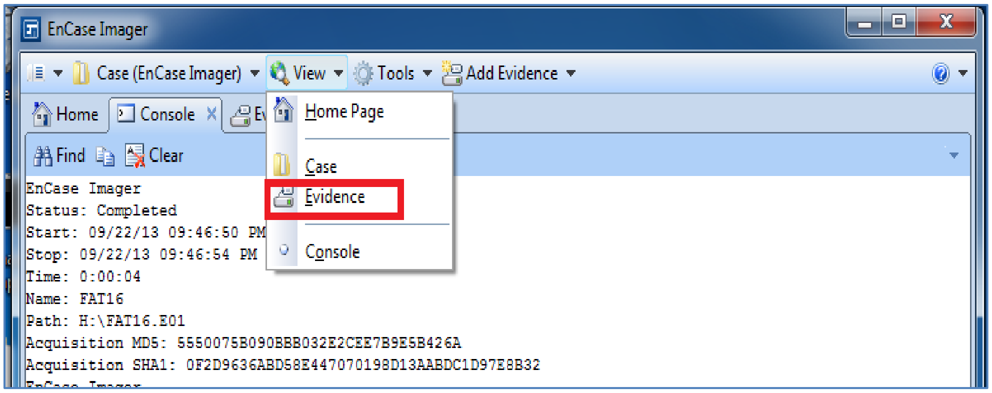


16. View the MD5 and SHA1 hashes, along with the date and time of the acquisition.



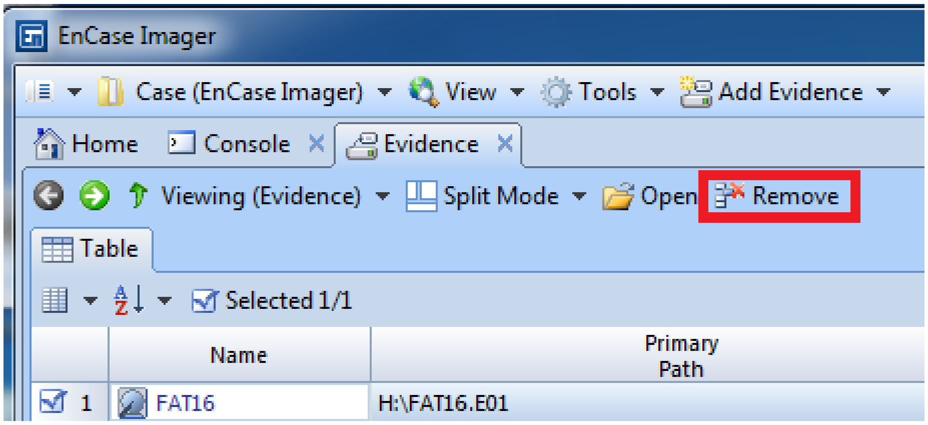
```
EnCase Imager
Status: Completed
Start: 05/06/14 10:02:19 PM
Stop: 05/06/14 10:02:23 PM
Time: 0:00:04
Name: FAT16
Path: C:\Users\student\Documents\FAT16.E01
Acquisition MD5: F2C6A2EBEC582C8F5921025297273388
Acquisition SHA1: 9D920D37A7D0DE1C8A4006086AE8F3806F902AFB
EnCase Imager
Status: Completed
Start: 05/06/14 10:02:23 PM
Stop: 05/06/14 10:02:23 PM
Time: 0:00:00
FAT16: Verified, no errors
EnCase Imager
Status: Completed
Start: 05/06/14 10:04:48 PM
Stop: 05/06/14 10:04:50 PM
Time: 0:00:02
Name: FAT16
Path: H:\FAT16.E01
Acquisition MD5: F2C6A2EBEC582C8F5921025297273388
Acquisition SHA1: 9D920D37A7D0DE1C8A4006086AE8F3806F902AFB
EnCase Imager
Status: Completed
Start: 05/06/14 10:04:50 PM
```

17. Select View from the Menu bar and then select **Evidence** from the dropdown list.



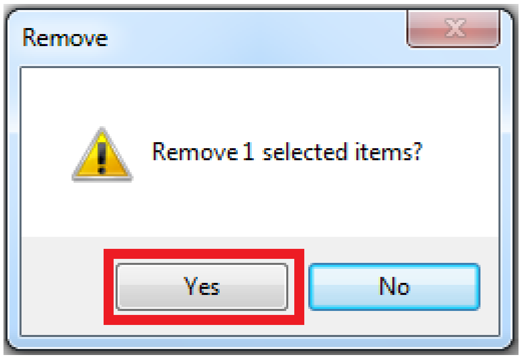
```
EnCase Imager
Status: Completed
Start: 09/22/13 09:46:50 PM
Stop: 09/22/13 09:46:54 PM
Time: 0:00:04
Name: FAT16
Path: H:\FAT16.E01
Acquisition MD5: 5550075B090BBB032E2CEE7B9E5B426A
Acquisition SHA1: 0F2D9636ABD58E447070198D13AABDC1D97E8B32
```

18. Verify that disk 1 is checked and then click the **Remove** button.



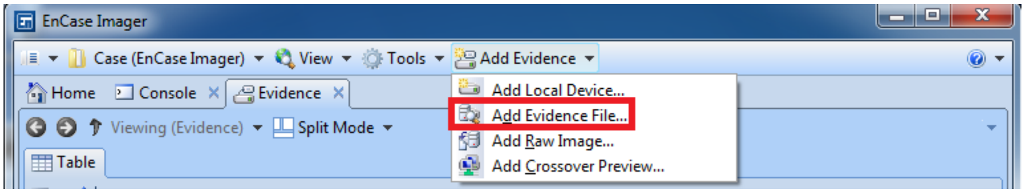
	Name	Primary Path
☑ 1	FAT16	H:\FAT16.E01

19. Click **Yes** when you are asked, *Remove 1 selected items?*

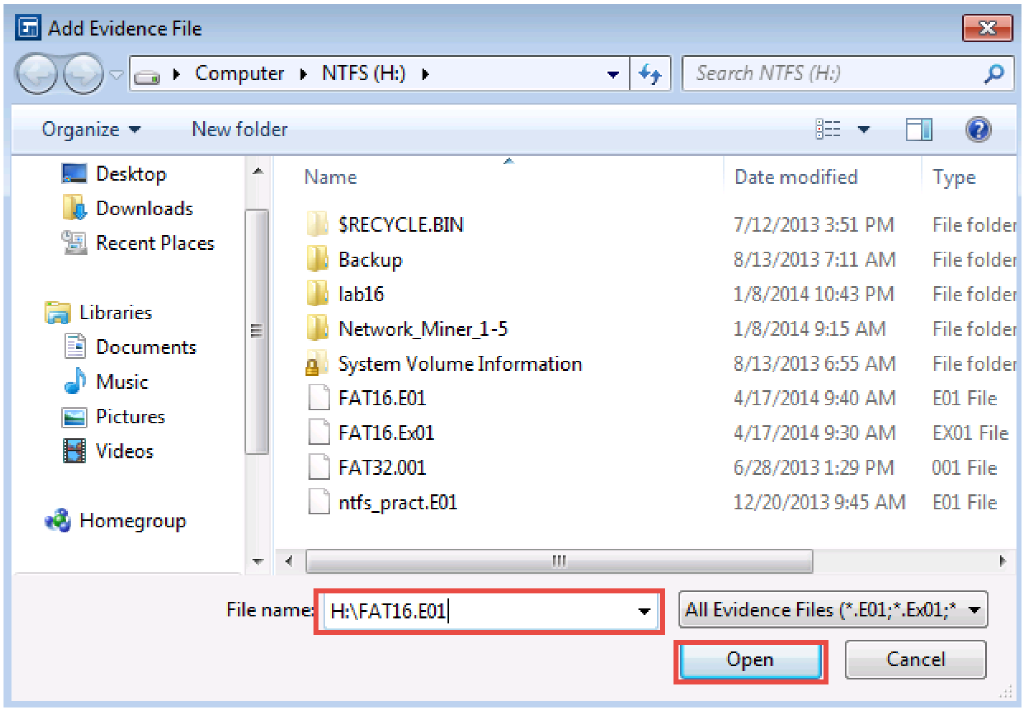


Remove 1 selected items?

20. Click the Add Evidence Drop-down box. Click **Add Evidence File**.



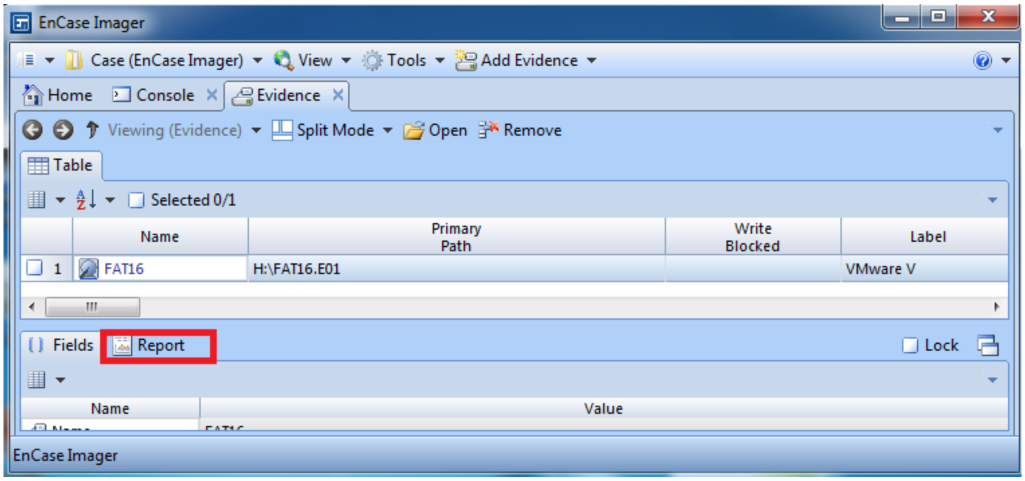
21. Type **H:\FAT16.E01** as the file name and click **Open** to load the image file into EnCase.



Name	Date modified	Type
$RECYCLE.BIN	7/12/2013 3:51 PM	File folder
Backup	8/13/2013 7:11 AM	File folder
lab16	1/8/2014 10:43 PM	File folder
Network_Miner_1-5	1/8/2014 9:15 AM	File folder
System Volume Information	8/13/2013 6:55 AM	File folder
FAT16.E01	4/17/2014 9:40 AM	E01 File
FAT16.Ex01	4/17/2014 9:30 AM	EX01 File
FAT32.001	6/28/2013 1:29 PM	001 File
ntfs_pract.E01	12/20/2013 9:45 AM	E01 File

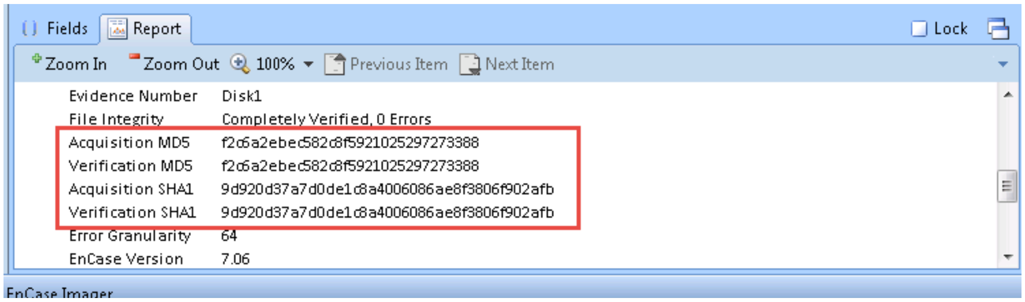
File name: H:\FAT16.E01

22. Click the **Report** tab so you can obtain information about the image hashes.



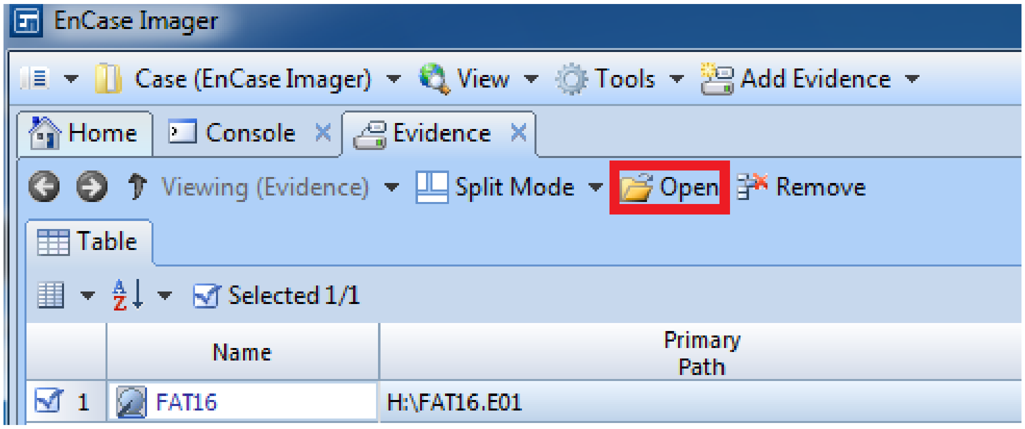
		Name	Primary Path	Write Blocked	Label
□	1	FAT16	H:\FAT16.E01		VMware V

23. View the MD5 and SHA1 Verification and Acquisition hashes within the report. (You may need to resize the report window.)



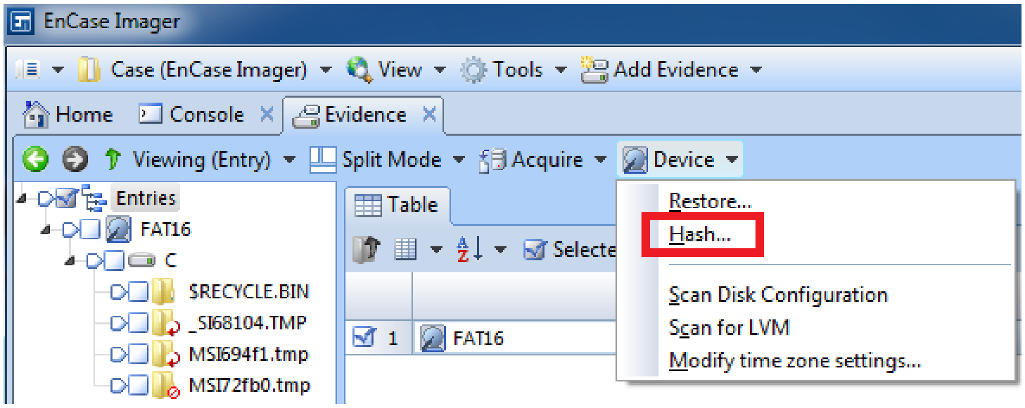
```
Evidence Number     Disk1
File Integrity      Completely Verified, 0 Errors
Acquisition MD5     f2c6a2ebec582c8f5921025297273388
Verification MD5    f2c6a2ebec582c8f5921025297273388
Acquisition SHA1    9d920d37a7d0de1c8a4006086ae8f3806f902afb
Verification SHA1   9d920d37a7d0de1c8a4006086ae8f3806f902afb
Error Granularity   64
EnCase Version      7.06
```

24. Verify that the disk is selected and click the **Open** button.

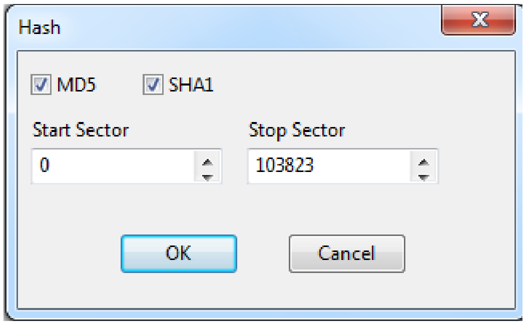


		Name	Primary Path
☑	1	FAT16	H:\FAT16.E01

25. From the Device menu within EnCase, select **Hash** from the menu list.



26. Leave the default options for the Hash window that appears. Click OK.

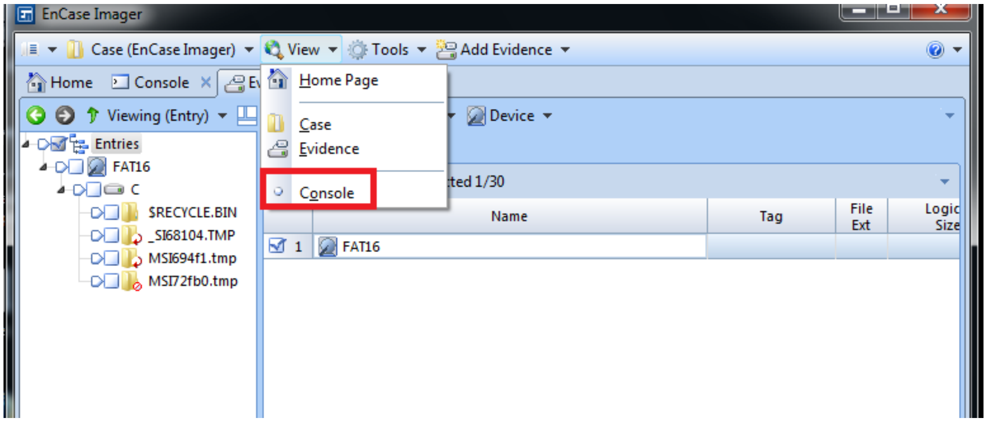

Hash

☑ MD5 ☑ SHA1

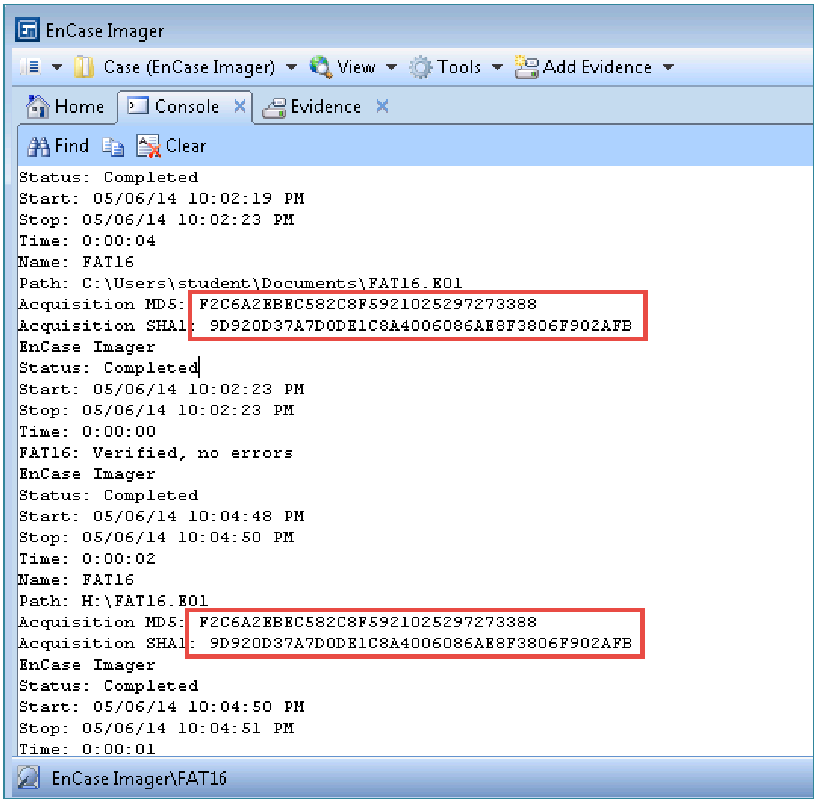
Start Sector: 0

Stop Sector: 103823

27. Select **Console** from the View menu, in order to view the hashes of the disk.



28. View the Verification Hashes. They should match the previous Acquisition hashes. Close all open windows.



```
Status: Completed
Start: 05/06/14 10:02:19 PM
Stop: 05/06/14 10:02:23 PM
Time: 0:00:04
Name: FAT16
Path: C:\Users\student\Documents\FAT16.E01
Acquisition MD5: F2C6A2EBEC582C8F5921025297273388
Acquisition SHA1: 9D920D37A7D0DE1C8A4006086AE8F3806F902AFB
EnCase Imager
Status: Completed
Start: 05/06/14 10:02:23 PM
Stop: 05/06/14 10:02:23 PM
Time: 0:00:00
FAT16: Verified, no errors
EnCase Imager
Status: Completed
Start: 05/06/14 10:04:48 PM
Stop: 05/06/14 10:04:50 PM
Time: 0:00:02
Name: FAT16
Path: H:\FAT16.E01
Acquisition MD5: F2C6A2EBEC582C8F5921025297273388
Acquisition SHA1: 9D920D37A7D0DE1C8A4006086AE8F3806F902AFB
EnCase Imager
Status: Completed
Start: 05/06/14 10:04:50 PM
Stop: 05/06/14 10:04:51 PM
Time: 0:00:01
```

EnCase Imager\FAT16

1.2 Conclusion

EnCase Imager is a GUI Program that will allow a user to create a disk image from within Windows. You can choose to use the MD5 or SHA1 hash, or you can use both hashes. The examiner will hash the disk image after loading it and verify the acquisition hashes.

1.3 Discussion Questions

1. What company makes EnCase Imager?
2. EnCase allows you to create disk images in which two formats?
3. What are the two hashing algorithms that EnCase Imager supports?
4. Which sections of EnCase Imager allow you to view information about hashes

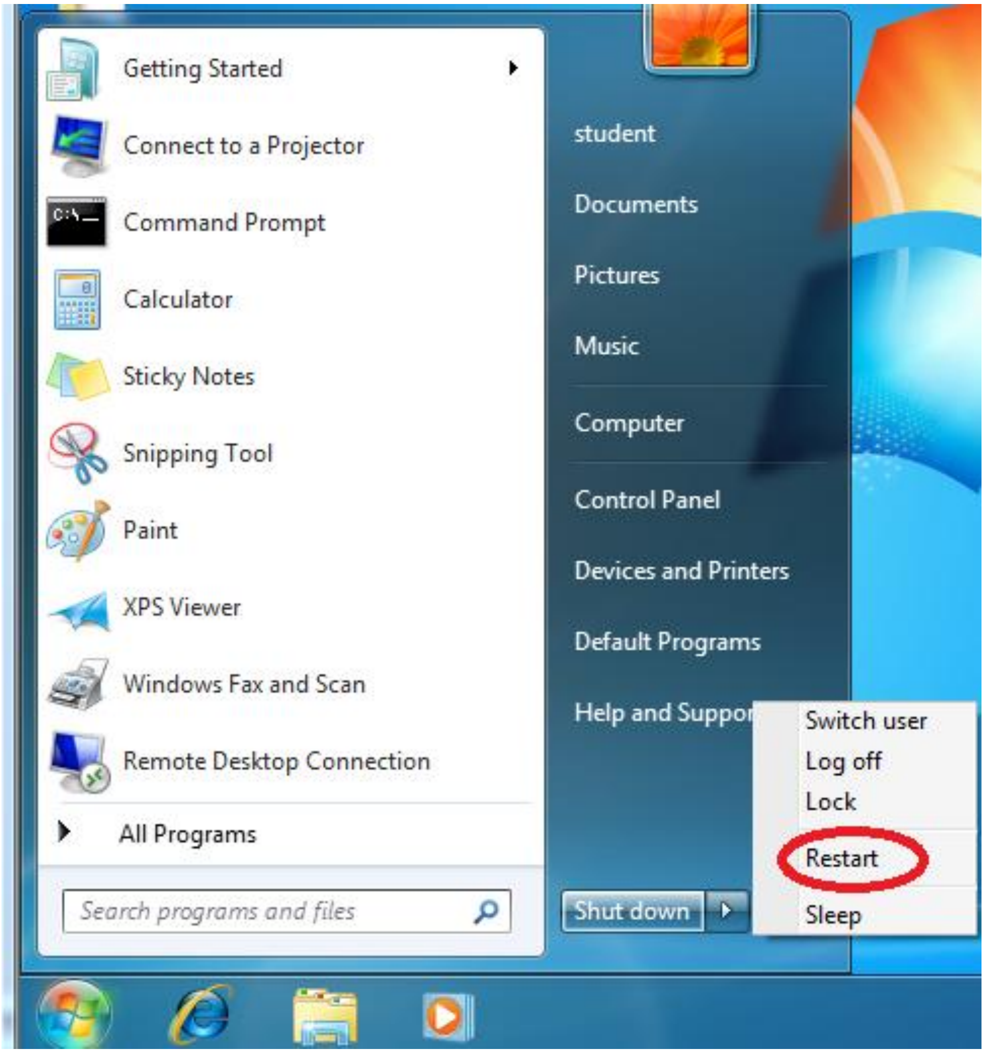
2 Using BackTrack to Hash Images, Disks, and Partitions

BackTrack is a free Ubuntu Linux-based Live DVD. BackTrack, from Offensive-Security, is used for forensics and penetration testing. It is available for download at the following link: http://www.backtrack-linux.org/downloads/. The BackTrack DVD, like HELIX, does not automatically mount disks. When disks are automatically mounted, it is possible that they can be written to, possibly resulting in the contamination of evidence.

2.1 Using BackTrack

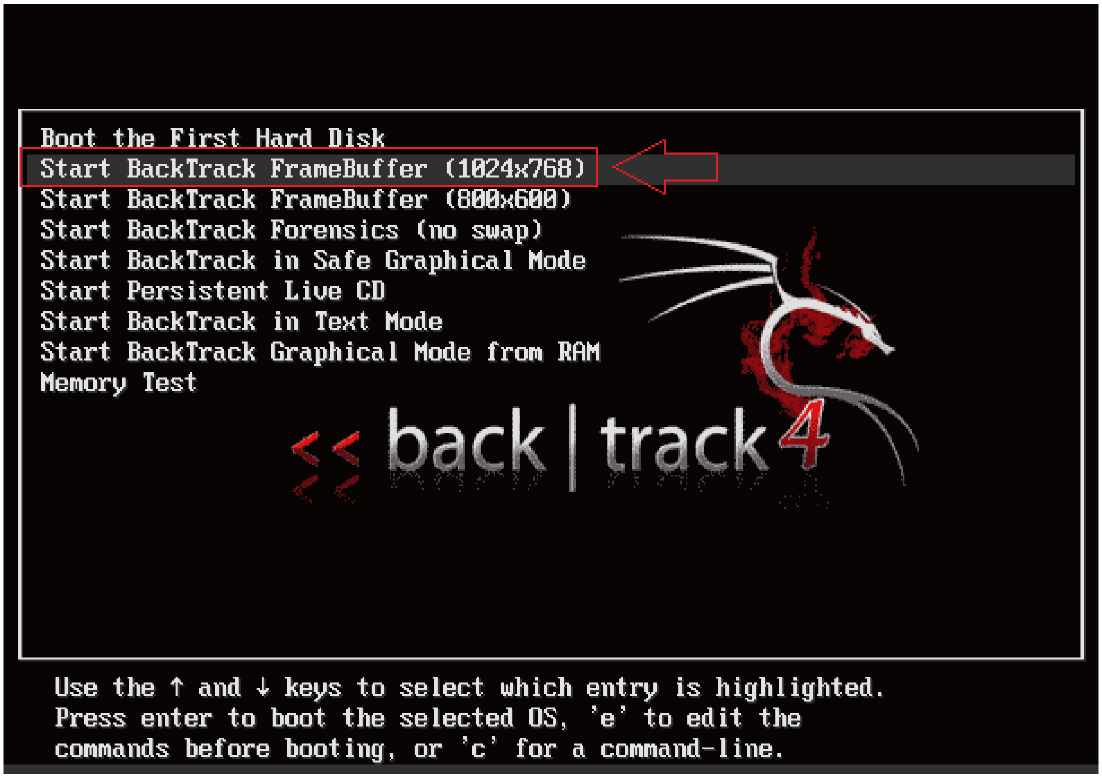
Perform the following steps on the Windows 7 External Machine.

1. Click Start, click the arrow to the right of Shutdown and then click **Restart**.



The machine will be booting to a Linux Live DVD Distribution (BackTrack). A Live DVD is an operating system that runs completely in Random Access Memory (RAM).

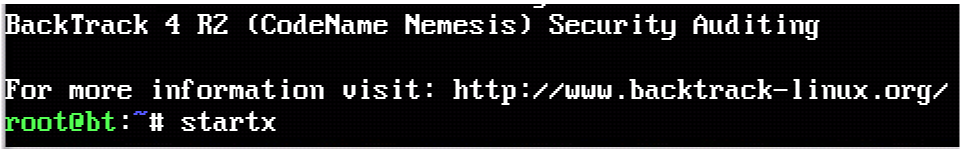
2. Choose the second choice on the boot menu. Press **Enter.**



```
Boot the First Hard Disk
Start BackTrack FrameBuffer (1024x768)
Start BackTrack FrameBuffer (800x600)
Start BackTrack Forensics (no swap)
Start BackTrack in Safe Graphical Mode
Start Persistent Live CD
Start BackTrack in Text Mode
Start BackTrack Graphical Mode from RAM
Memory Test

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
```

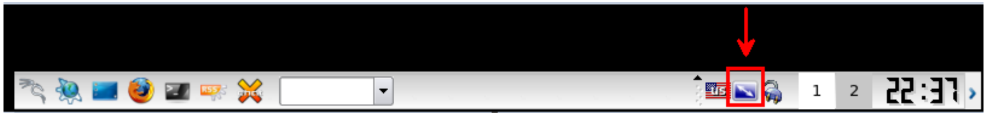
3. After BackTrack boots, type the following command to initialize the GUI. root@bt:~# **startx.** If you get a message saying the connection to the virtual machine was lost, click **YES** to reconnect.



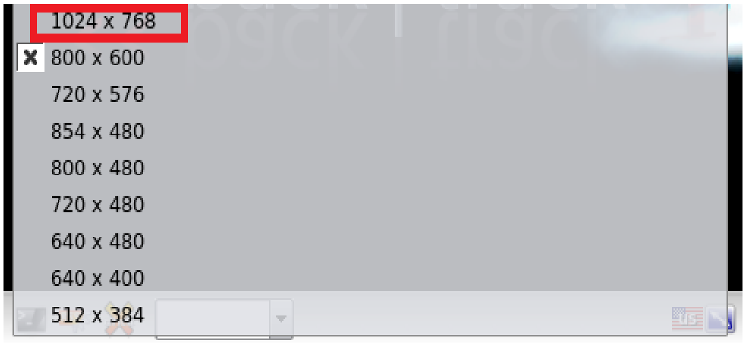
```
BackTrack 4 R2 (CodeName Nemesis) Security Auditing

For more information visit: http://www.backtrack-linux.org/
root@bt:~# startx
```

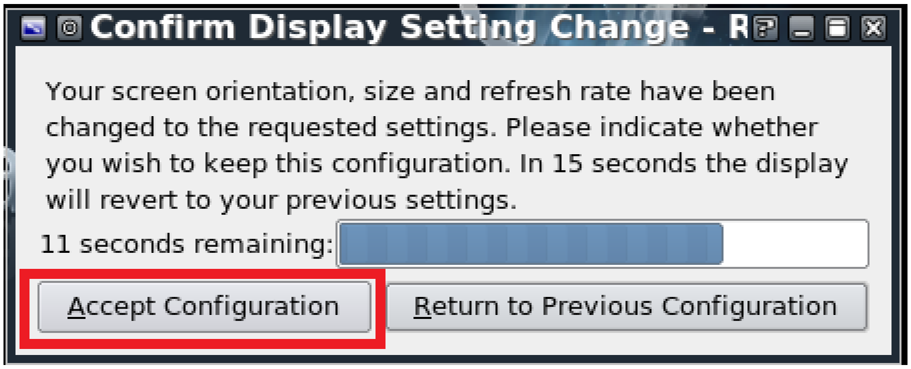
4. You can adjust the resolution by clicking on the blue arrows to the right of US.



5. Select the resolution of your choice to use on the virtual machine.



6. Click **Accept Configuration** to accept the Display Settings change.

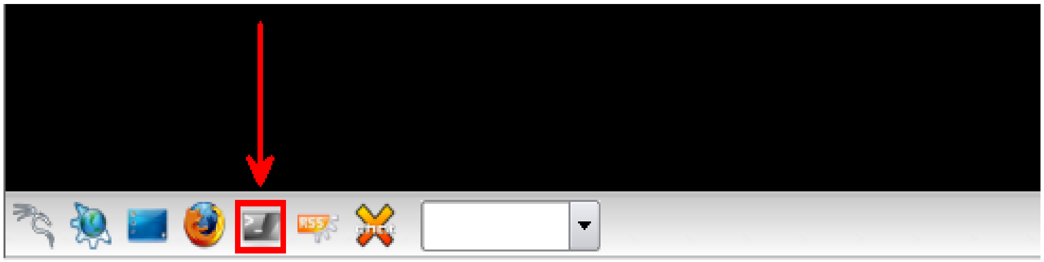

Confirm Display Setting Change - R

Your screen orientation, size and refresh rate have been changed to the requested settings. Please indicate whether you wish to keep this configuration. In 15 seconds the display will revert to your previous settings.

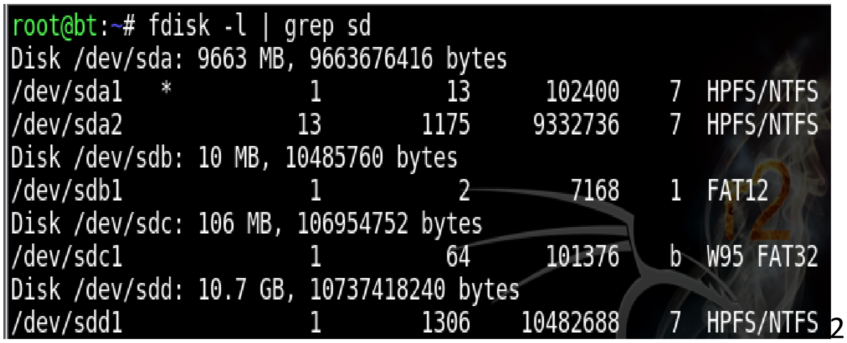
11 seconds remaining:

Accept Configuration
Return to Previous Configuration

7. Open a terminal on the Linux system by clicking on the black square icon (to the right of Firefox) in the task bar, at the bottom of the BackTrack desktop.



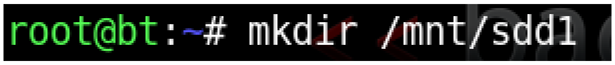
8. Type the following to display the disks and their corresponding partitions:
root@bt:~# **fdisk –l | grep sd**



```
root@bt:~# fdisk -l | grep sd
Disk /dev/sda: 9663 MB, 9663676416 bytes
/dev/sda1   *           1          13      102400    7  HPFS/NTFS
/dev/sda2              13        1175     9332736    7  HPFS/NTFS
Disk /dev/sdb: 10 MB, 10485760 bytes
/dev/sdb1               1           2        7168    1  FAT12
Disk /dev/sdc: 106 MB, 106954752 bytes
/dev/sdc1               1          64      101376    b  W95 FAT32
Disk /dev/sdd: 10.7 GB, 10737418240 bytes
/dev/sdd1               1        1306    10482688    7  HPFS/NTFS
```
2

We need to mount our destination media so we can send images and hashes to it.

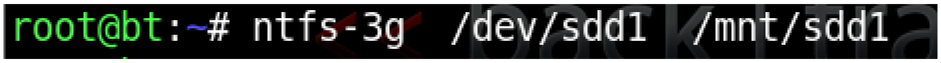
9. Type the following to make a directory called sdd1 in the /mnt directory:
   root@bt:~# **mkdir /mnt/sdd1**



```
root@bt:~# mkdir /mnt/sdd1
```

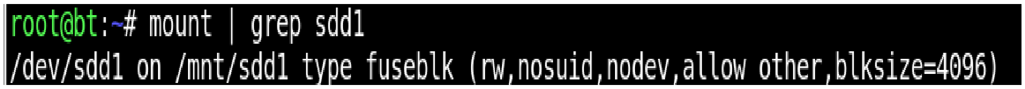
Next, we will mount the sdd1 partition to the /mnt/sdd1 directory we created.

10. Type the following command to mount the NTFS partition:
    root@bt:~# **ntfs-3g /dev/sdd1 /mnt/sdd1**



```
root@bt:~# ntfs-3g  /dev/sdd1  /mnt/sdd1
```

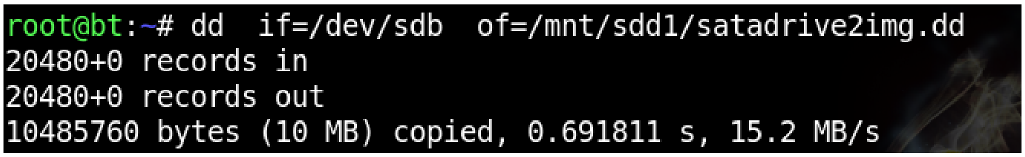
11. Type the following command to view the newly mounted partition:
    root@bt:~# **mount | grep sdd1**



```
root@bt:~# mount | grep sdd1
/dev/sdd1 on /mnt/sdd1 type fuseblk (rw,nosuid,nodev,allow other,blksize=4096)
```

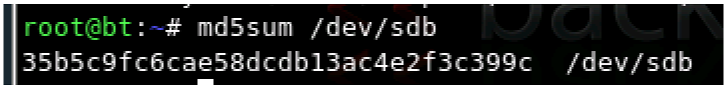
In the next step, we will make an image of the second SATA disk and send it to our destination drive, the 4th SATA drive that is the mounted NTFS data drive.

12. To make a copy of the second SATA drive using dd, type the following:
    root@bt:~#



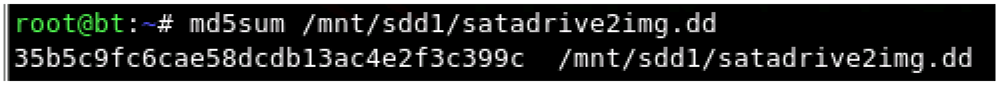
```
root@bt:~# dd  if=/dev/sdb  of=/mnt/sdd1/satadrive2img.dd
20480+0 records in
20480+0 records out
10485760 bytes (10 MB) copied, 0.691811 s, 15.2 MB/s
```

13. Next, we will hash the files of the second SATA disk using the md5sum command:
    root@bt:~# **md5sum /dev/sdb**



```
root@bt:~# md5sum /dev/sdb
35b5c9fc6cae58dcdb13ac4e2f3c399c  /dev/sdb
```

14. Now, we will hash the disk image we created using the md5sum command:
    root@bt:~# **md5sum /mnt/sdd1/satadrive2img.dd**

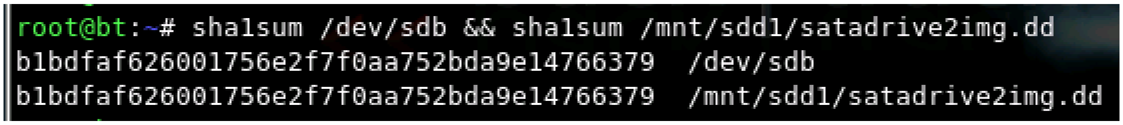


```
root@bt:~# md5sum /mnt/sdd1/satadrive2img.dd
35b5c9fc6cae58dcdb13ac4e2f3c399c  /mnt/sdd1/satadrive2img.dd
```

The hashes match. This means the disk and image file are forensically equivalent.

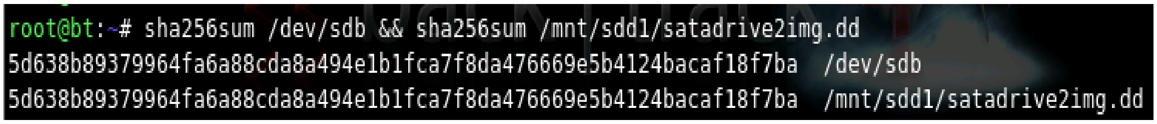
Next, we will use the SHA1 hash, which is a 160 bit value, and more accurate than MD5.

15. Using the SHA1 hash, both devices can be hashed at the same time by typing the following command:
    root@bt:~# **sha1sum /dev/sdb   &&   sha1sum /mnt/sdd1/satadrive2img.dd**



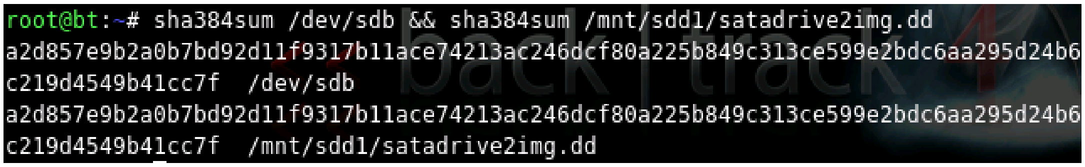
```
root@bt:~# sha1sum /dev/sdb && sha1sum /mnt/sdd1/satadrive2img.dd
b1bdfaf626001756e2f7f0aa752bda9e14766379  /dev/sdb
b1bdfaf626001756e2f7f0aa752bda9e14766379  /mnt/sdd1/satadrive2img.dd
```

16. Using the SHA256 hash, both devices can be hashed at the same time by typing the following command:
    root@bt:~#**sha256sum /dev/sdb && sha256sum /mnt/sdd1/satadrive2img.dd**



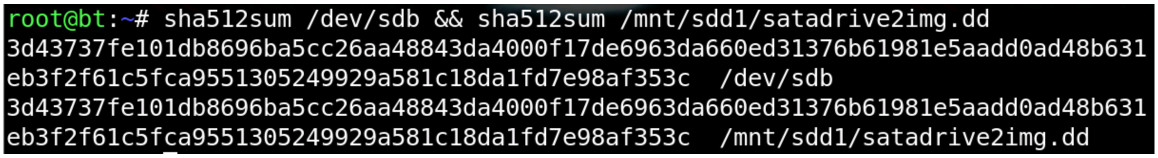
```
root@bt:~# sha256sum /dev/sdb && sha256sum /mnt/sdd1/satadrive2img.dd
5d638b89379964fa6a88cda8a494e1b1fca7f8da476669e5b4124bacaf18f7ba  /dev/sdb
5d638b89379964fa6a88cda8a494e1b1fca7f8da476669e5b4124bacaf18f7ba  /mnt/sdd1/satadrive2img.dd
```

17. Using the SHA384 hash, both devices can be hashed at the same time by typing the following command:
    root@bt:~#**sha384sum /dev/sdb && sha384sum /mnt/sdd1/satadrive2img.dd**



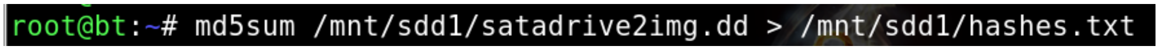
```
root@bt:~# sha384sum /dev/sdb && sha384sum /mnt/sdd1/satadrive2img.dd
a2d857e9b2a0b7bd92d11f9317b11ace74213ac246dcf80a225b849c313ce599e2bdc6aa295d24b6
c219d4549b41cc7f  /dev/sdb
a2d857e9b2a0b7bd92d11f9317b11ace74213ac246dcf80a225b849c313ce599e2bdc6aa295d24b6
c219d4549b41cc7f  /mnt/sdd1/satadrive2img.dd
```

18. Using the SHA512 hash, both devices can be hashed at the same time by typing the following command:
    root@bt:~#**sha512sum /dev/sdb && sha512sum /mnt/sdd1/satadrive2img.dd**



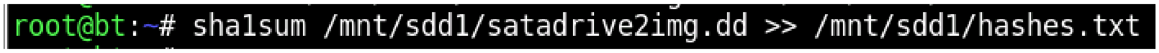
```
root@bt:~# sha512sum /dev/sdb && sha512sum /mnt/sdd1/satadrive2img.dd
3d43737fe101db8696ba5cc26aa48843da4000f17de6963da660ed31376b61981e5aadd0ad48b631
eb3f2f61c5fca9551305249929a581c18da1fd7e98af353c  /dev/sdb
3d43737fe101db8696ba5cc26aa48843da4000f17de6963da660ed31376b61981e5aadd0ad48b631
eb3f2f61c5fca9551305249929a581c18da1fd7e98af353c  /mnt/sdd1/satadrive2img.dd
```

19. Send the MD5 hash of the image file to a text file named hashes by typing:
    root@bt:~# **md5sum /mnt/sdd1/satadrive2img.dd > /mnt/sdd1/hashes.txt**



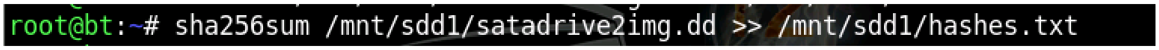
```
root@bt:~# md5sum /mnt/sdd1/satadrive2img.dd > /mnt/sdd1/hashes.txt
```

20. Send the SHA1 hash of the image file to a text file called hashes by typing:
    root@bt:~# **sha1sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt**



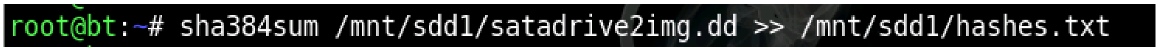
```
root@bt:~# sha1sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt
```

21. Send the SHA256 hash of the image file to a text file called hashes by typing:
    root@bt:~# **sha256sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt**



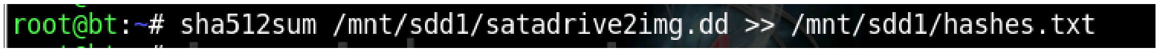
```
root@bt:~# sha256sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt
```

22. Send the SHA384 hash of the image file to a text file called hashes by typing:
    root@bt:~# **sha384sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt**



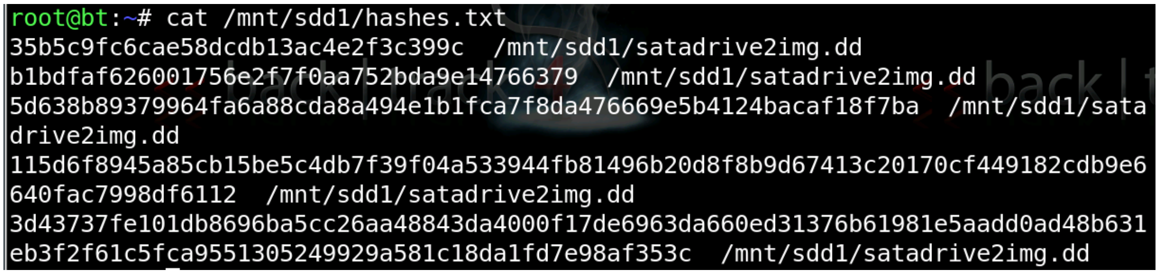
```
root@bt:~# sha384sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt
```

23. Send the SHA512 hash of the image file to a text file called hashes by typing:
    root@bt:~# **sha512sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt**



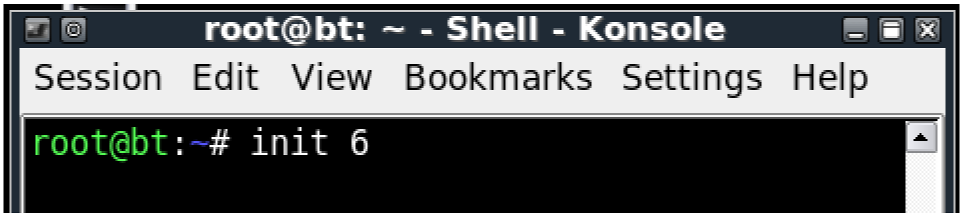
```
root@bt:~# sha512sum /mnt/sdd1/satadrive2img.dd >> /mnt/sdd1/hashes.txt
```

24. View the contents of the hashes.txt file you created by typing:
    root@bt:~#**cat /mnt/sdd1/hashes.txt**



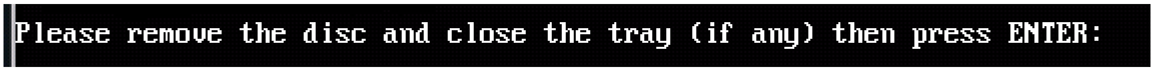
```
root@bt:~# cat /mnt/sdd1/hashes.txt
35b5c9fc6cae58dcdb13ac4e2f3c399c  /mnt/sdd1/satadrive2img.dd
b1bdfaf626001756e2f7f0aa752bda9e14766379  /mnt/sdd1/satadrive2img.dd
5d638b89379964fa6a88cda8a494e1b1fca7f8da476669e5b4124bacaf18f7ba  /mnt/sdd1/sata
drive2img.dd
115d6f8945a85cb15be5c4db7f39f04a533944fb81496b20d8f8b9d67413c20170cf449182cdb9e6
640fac7998df6112  /mnt/sdd1/satadrive2img.dd
3d43737fe101db8696ba5cc26aa48843da4000f17de6963da660ed31376b61981e5aadd0ad48b631
eb3f2f61c5fca9551305249929a581c18da1fd7e98af353c  /mnt/sdd1/satadrive2img.dd
```

25. Type the following command to unmount all disks and reboot the system:
    root@bt:~#**init 6**



```
root@bt:~# init 6
```

26. Press Enter when you receive the message to remove the disk.



```
Please remove the disc and close the tray (if any) then press ENTER:
```

2.2 Conclusion

BackTrack can be used as a Live DVD to perform forensic acquisitions with the dd or dcfldd command. After acquiring a disk image, the image and the original disk can be hashed to verify that there data sets are forensically equivalent. Commands like md5sum, sha1sum, sha256sum, sha384, and sha512sum can be used for hashing.

2.3 Discussion Questions

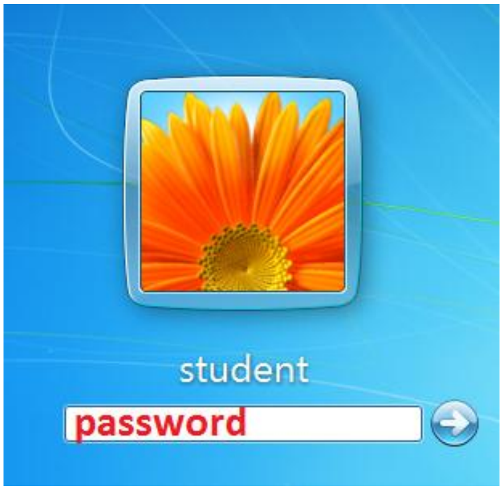
1. What is BackTrack?
2. What is a Live DVD?
3. What are the different sha commands available within BackTrack for hashing?
4. What command can be used to verify that disks are mounted within Linux?

3 Using HashCalc to Verify Hashes

The md5sum, sha1sum, sha256sum, sha384, and sha512sum commands in BackTrack can be used for hashing. However, not everyone is comfortable with using the terminal within Linux to run commands. There are GUI based tools, such as HashCalc, that will allow an examiner to hash files within Windows without typing commands at the command prompt.

3.1 Installing and Using HashCalc

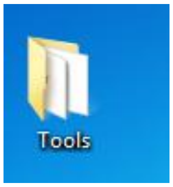
1. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password,** and press **Enter** to log in.



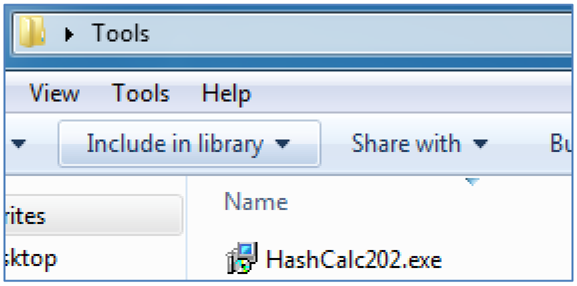
student

password

4. Double-click on the **Tools** folder on the desktop.

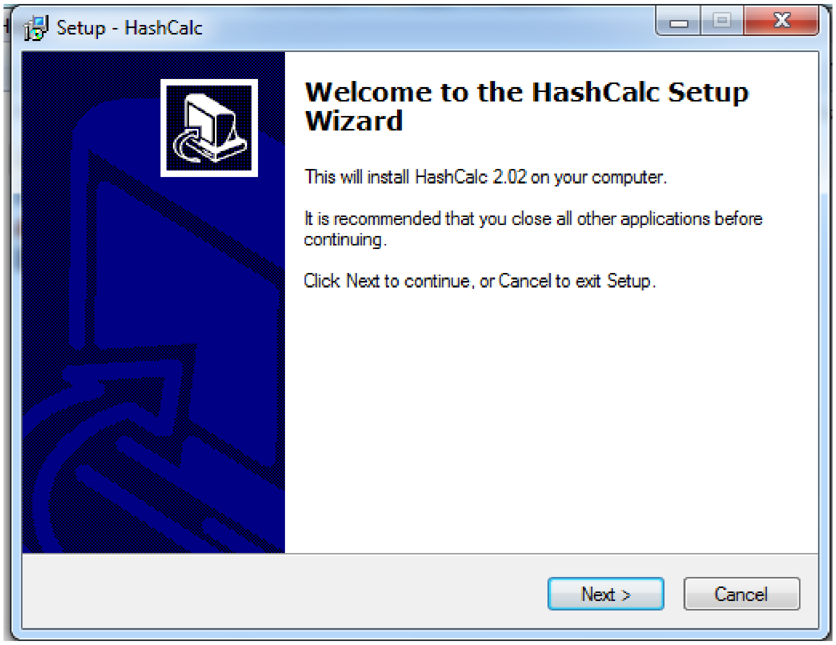


5. Double-click on the **HashCalc202.exe** file in the Tools folder.



HashCalc202.exe

6. Click **Next** at the Welcome to the HashCalc Setup Wizard screen.



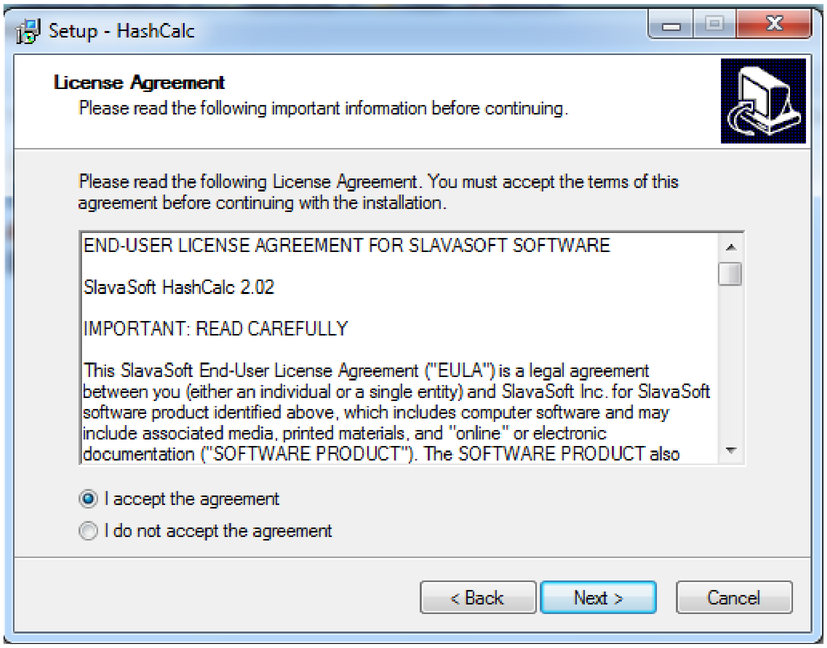
Welcome to the HashCalc Setup Wizard

This will install HashCalc 2.02 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

7. Select the **I accept the agreement** box and click Next.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

END-USER LICENSE AGREEMENT FOR SLAVASOFT SOFTWARE

SlavaSoft HashCalc 2.02

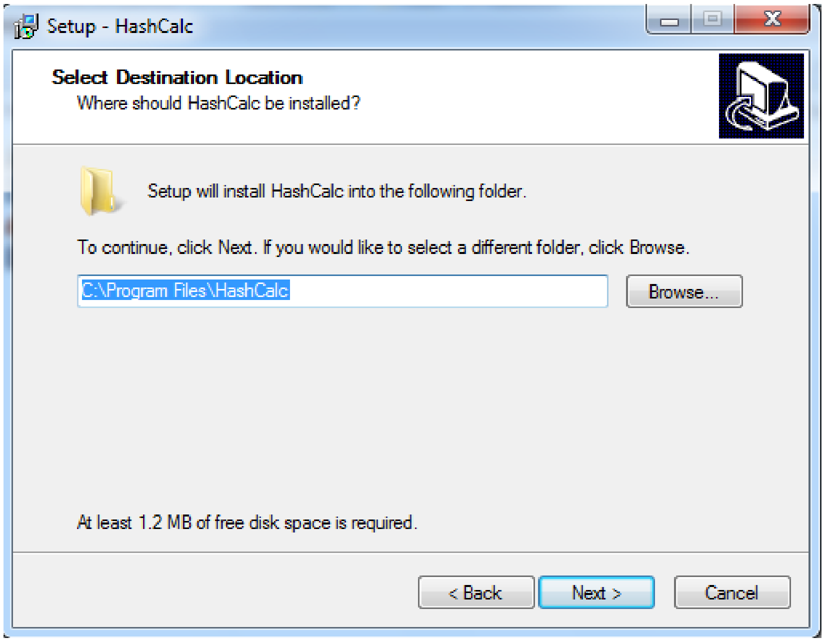
IMPORTANT: READ CAREFULLY

This SlavaSoft End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and SlavaSoft Inc. for SlavaSoft software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE PRODUCT also

● I accept the agreement

○ I do not accept the agreement

8. Accept the default location for the installation and click Next.



Select Destination Location

Where should HashCalc be installed?

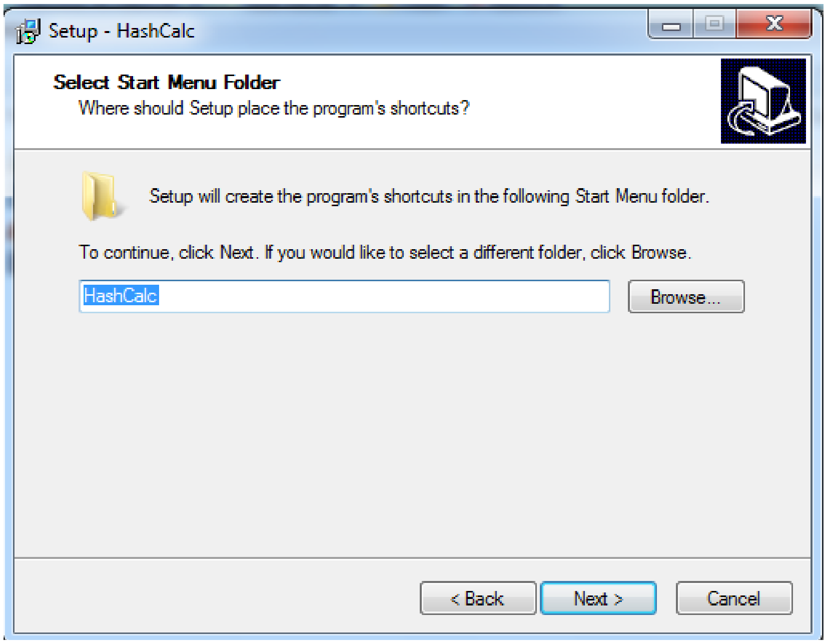
Setup will install HashCalc into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\HashCalc

At least 1.2 MB of free disk space is required.

9. Click Next at the **Select Start Menu Folder** screen.



Select Start Menu Folder

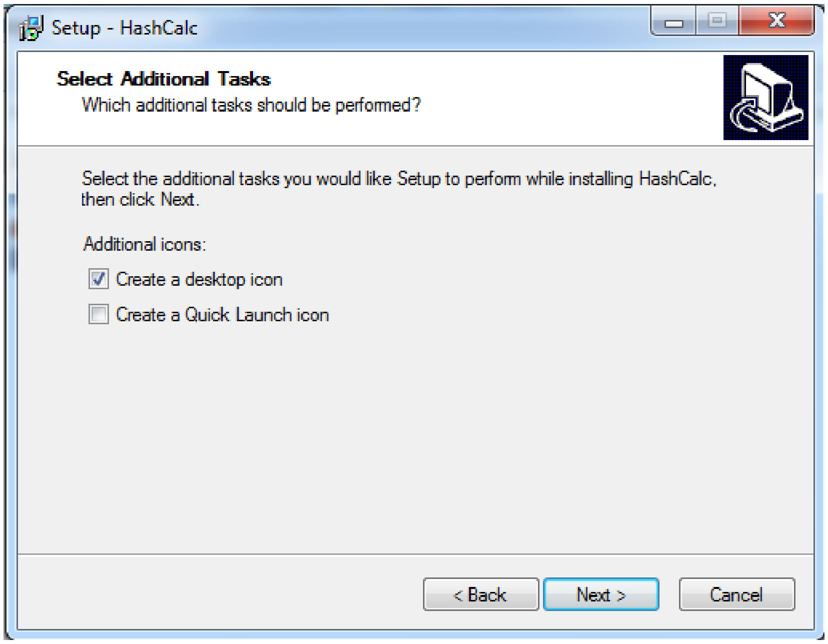
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

HashCalc

10. Accept the default choices at the **Select Additional Tasks** screen.



Setup - HashCalc

Select Additional Tasks

Which additional tasks should be performed?

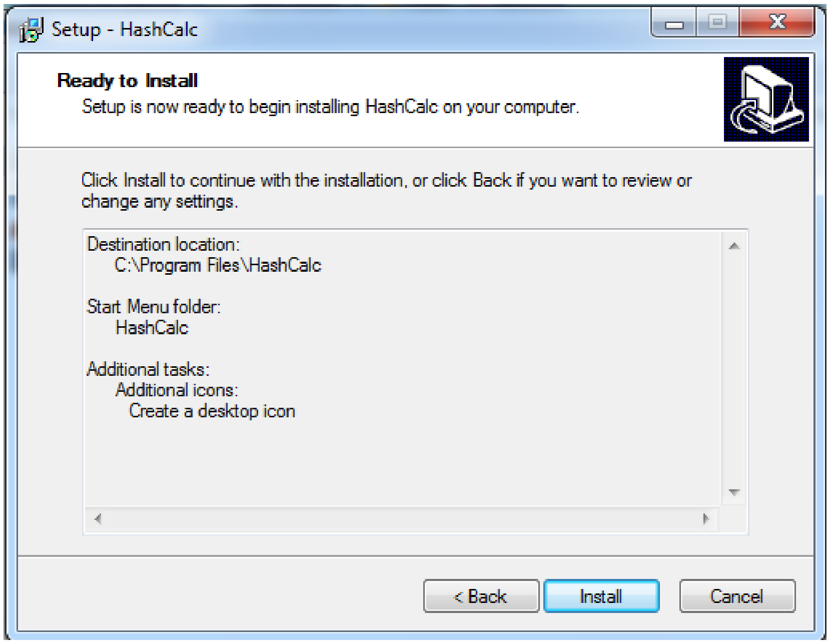
Select the additional tasks you would like Setup to perform while installing HashCalc, then click Next.

Additional icons:

☑ Create a desktop icon

□ Create a Quick Launch icon

11. Click the Install button at the **Ready to Install** screen.



Setup - HashCalc

Ready to Install

Setup is now ready to begin installing HashCalc on your computer.

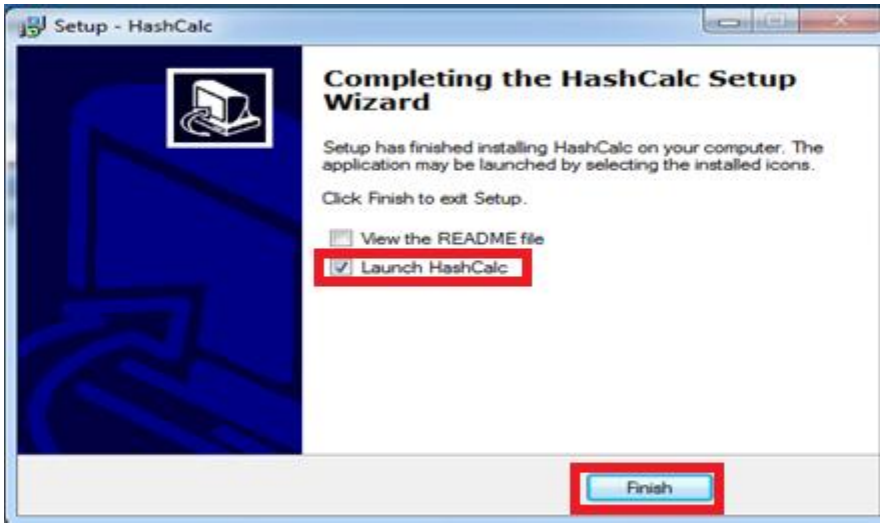
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
    C:\Program Files\HashCalc

Start Menu folder:
    HashCalc

Additional tasks:
    Additional icons:
      Create a desktop icon

12. At the Completing the HashCalc Setup Wizard Screen, uncheck the View the README file checkbox. Verify **Launch HashCalc** is checked and click **Finish**. Close the Tools Folder.



Completing the HashCalc Setup Wizard

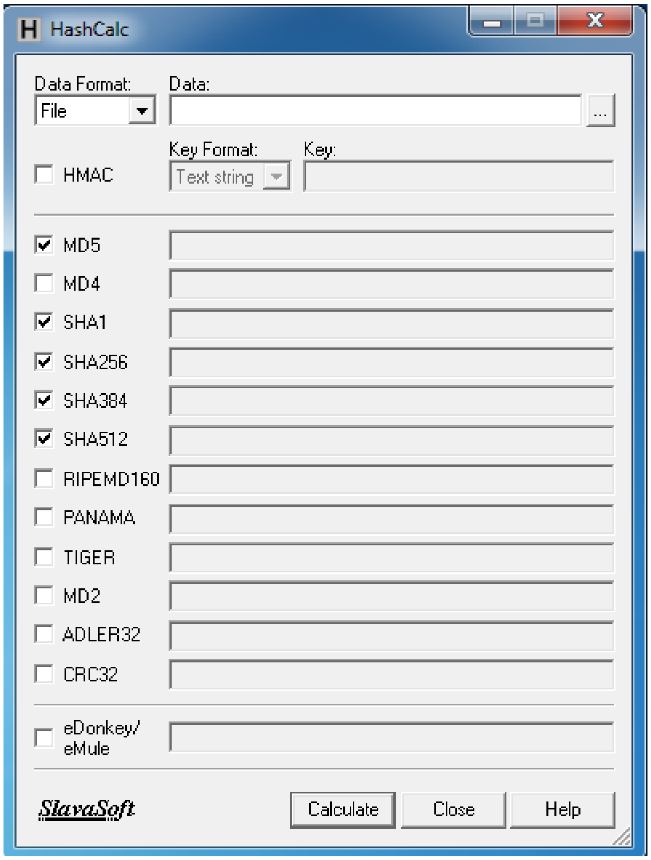
Setup has finished installing HashCalc on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

□ View the README file

☑ Launch HashCalc

13. On the HashCalc screen, check only MD5, SHA1, SHA256, SHA384, and SHA512.



Data Format: File

Data:

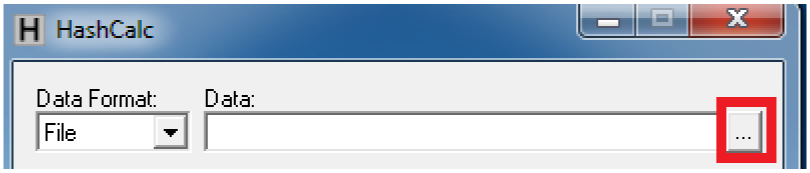
□ HMAC

Key Format: Text string

Key:

☑ MD5
□ MD4
☑ SHA1
☑ SHA256
☑ SHA384
☑ SHA512
□ RIPEMD160
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
□ CRC32
□ eDonkey/ eMule

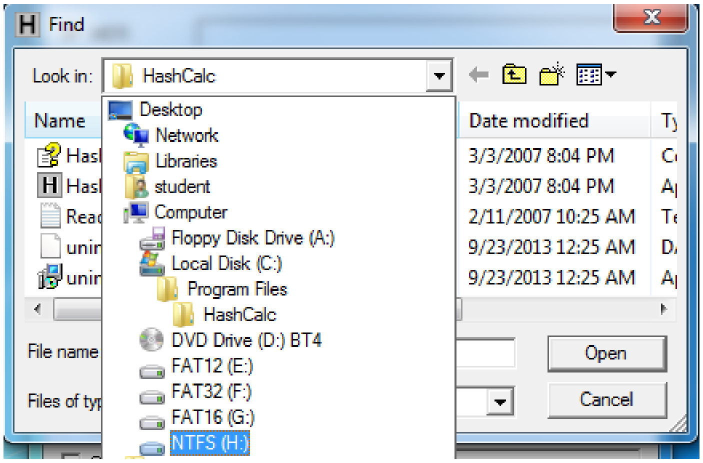
14. Click the browse button within the HashCalc program.



Data Format: File

Data:

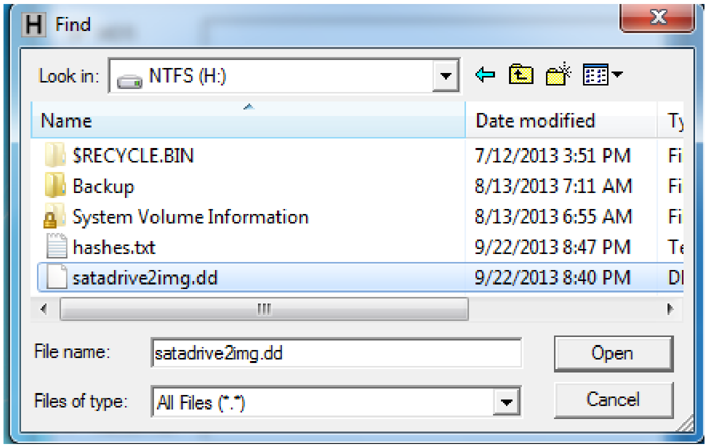
15. Click the **Look in** drop-down box and select **NTFS(H:)** from the list.



Look in: HashCalc

Name	Date modified	Ty
Hasl	3/3/2007 8:04 PM	C
Hasl	3/3/2007 8:04 PM	A
Read	2/11/2007 10:25 AM	Te
unir	9/23/2013 12:25 AM	D
unir	9/23/2013 12:25 AM	A

16. Double-click on the **satadrive2img.dd** file located on the NTFS(H:) drive.



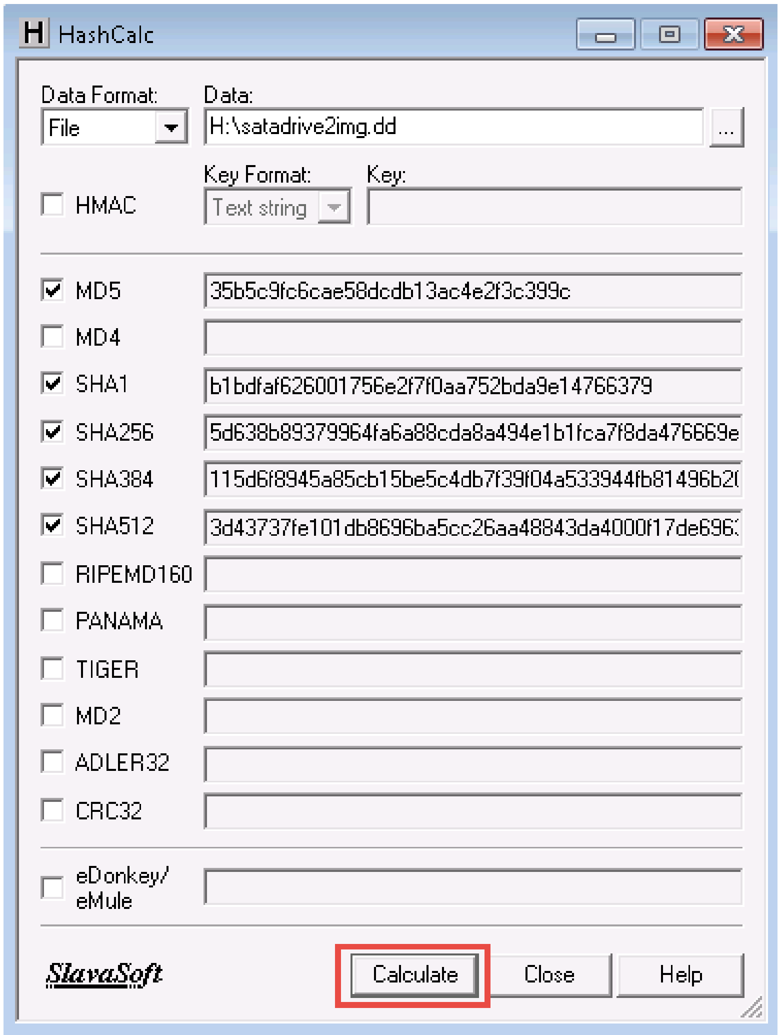
Look in: NTFS (H:)

Name	Date modified	Ty
$RECYCLE.BIN	7/12/2013 3:51 PM	Fi
Backup	8/13/2013 7:11 AM	Fi
System Volume Information	8/13/2013 6:55 AM	Fi
hashes.txt	9/22/2013 8:47 PM	Te
satadrive2img.dd	9/22/2013 8:40 PM	DI

File name: satadrive2img.dd

Files of type: All Files (*.*)

17. Click the **Calculate** button to calculate all of the hashes.



HashCalc

Data Format: File

Data: H:\satadrive2img.dd

□ HMAC Key Format: Text string Key:

☑ MD5 35b5c9fc6cae58dcdb13ac4e2f3c399c

□ MD4

☑ SHA1 b1bdfaf626001756e2f7f0aa752bda9e14766379

☑ SHA256 5d638b89379964fa6a88cda8a494e1b1fca7f8da476669e

☑ SHA384 115d6f8945a85cb15be5c4db7f39f04a533944fb81496b2

☑ SHA512 3d43737fe101db8696ba5cc26aa48843da4000f17de696

□ RIPEMD160

□ PANAMA

□ TIGER

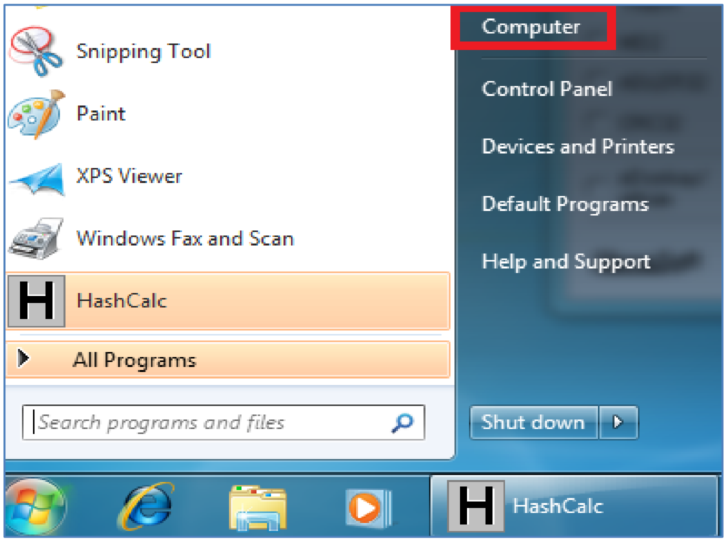
□ MD2

□ ADLER32

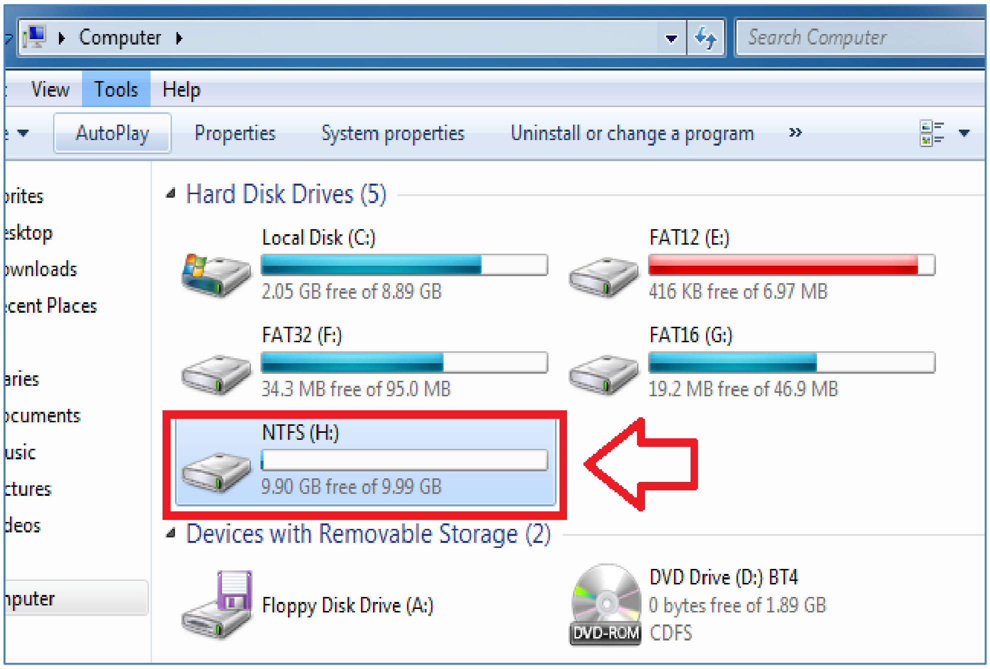
□ CRC32

□ eDonkey/ eMule

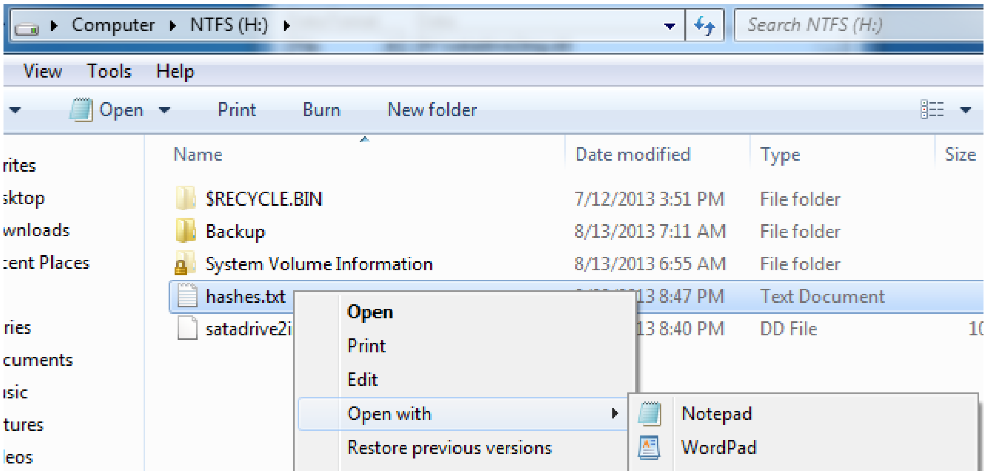
18. Click on the Start button and then click on **Computer.**



19. Double-click on the **NTFS (H:)** drive on the list.

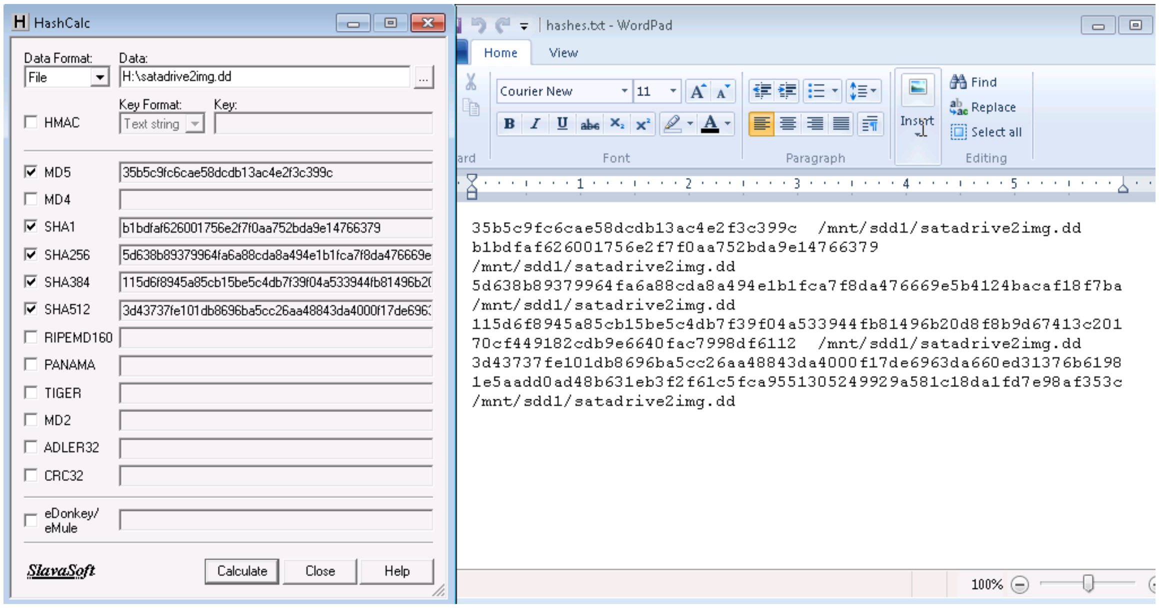


20. Right-click on the hashes.txt file and select **Open with > WordPad.**



Name	Date modified	Type	Size
$RECYCLE.BIN	7/12/2013 3:51 PM	File folder	
Backup	8/13/2013 7:11 AM	File folder	
System Volume Information	8/13/2013 6:55 AM	File folder	
hashes.txt	13 8:47 PM	Text Document	
satadrive2i	13 8:40 PM	DD File	1(

21. Compare all of the hashes from HashCalc and hashes.txt. They are the same. Close all open windows and the Windows 7 PC Viewer.



Data Format: File

Data: H:\satadrive2img.dd

☐ HMAC   Key Format: Text string   Key:

☑ MD5 35b5c9fc6cae58dcdb13ac4e2f3c399c

☐ MD4

☑ SHA1 b1bdfaf626001756e2f7f0aa752bda9e14766379

☑ SHA256 5d638b89379964fa6a88cda8a494e1b1fca7f8da476669e

☑ SHA384 115d6f8945a85cb15be5c4db7f39f04a533944fb81496b2(

☑ SHA512 3d43737fe101db8696ba5cc26aa48843da4000f17de696:

☐ RIPEMD160

☐ PANAMA

☐ TIGER

☐ MD2

☐ ADLER32

☐ CRC32

☐ eDonkey/ eMule

```
35b5c9fc6cae58dcdb13ac4e2f3c399c  /mnt/sdd1/satadrive2img.dd
b1bdfaf626001756e2f7f0aa752bda9e14766379
/mnt/sdd1/satadrive2img.dd
5d638b89379964fa6a88cda8a494e1b1fca7f8da476669e5b4124bacaf18f7ba
/mnt/sdd1/satadrive2img.dd
115d6f8945a85cb15be5c4db7f39f04a533944fb81496b20d8f8b9d67413c201
70cf449182cdb9e6640fac7998df6112  /mnt/sdd1/satadrive2img.dd
3d43737fe101db8696ba5cc26aa48843da4000f17de6963da660ed31376b6198
1e5aadd0ad48b631eb3f2f61c5fca9551305249929a581c18da1fd7e98af353c
/mnt/sdd1/satadrive2img.dd
```

3.2 Conclusion

HashCalc is a free program from http://www.slavasoft.com/hashcalc/ that allows you to calculate the MD5, SHA256, SHA384, SHA512, and other hash values of data sets. After installing the program, you can browse to any file and calculate the hashes. Hashing data sets is a way to determine if a data set is forensically equivalent.

3.3 Discussion Questions

1. What does the HashCalc tool do?
2. What are some of the hashes that the HashCalc program will calculate?
3. What company makes the HashCalc Program?
4. Which SHA hash values does the HashCalc Program calculate?

References

1. BackTrack Linux:
   http://www.backtrack-linux.org/

2. EnCase Imager:
   https://www.guidancesoftware.com/pages/search.aspx?q=Forensics Imager

3. The dd Command:
   http://www.computerhope.com/unix/dd.htm

4. HashCalc:
   http://www.slavasoft.com/hashcalc/

5. MD5 Hash Explained:
   http://www.makeuseof.com/tag/md5-hash-stuff-means-technology-explained/