



DIGITAL FORENSICS LAB SERIES

Lab 5: The Imaging Process

Objective: Evidence Acquisition, Preparation and Preservation

Document Version: 2015-09-28



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

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 | 2 |
| Objective: Evidence Acquisition, Preparation and Preservation | 2 |
| Lab Topology | 3 |
| Lab Settings | 4 |
| 1 Using FTK Imager | 5 |
| 1.1 Imaging a Disk within Windows | 5 |
| 1.2 Conclusion | 17 |
| 1.3 Discussion Questions..... | 17 |
| 2 Using HELIX to Image a System..... | 18 |
| 2.1 Using HELIX..... | 18 |
| 2.2 Conclusion | 25 |
| 2.3 Discussion Questions..... | 25 |
| 3 Using BackTrack to Image a System..... | 26 |
| 3.1 Booting to the Live DVD Environment | 26 |
| 3.2 Conclusion | 30 |
| 3.3 Discussion Questions..... | 30 |
| References | 31 |



Introduction

This lab includes the following tasks:

1. Using FTK Imager
2. Using HELIX to Image a System
3. Using BackTrack to Image a System

Objective: Evidence Acquisition, Preparation and Preservation

Performing this lab will provide the student with a hands-on lab experience meeting the Evidence Acquisition, Preparation and Preservation Objective:

The candidate will demonstrate understanding of evidence chain-of-custody and integrity, E-discovery concepts, evidence acquisition and preservation, and the tools and techniques used by computer forensic examiners.

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 can be used to prove that the copy is forensically equivalent to the actual disk.

FTK Imager®– FTK 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. FTK Imager allows you to image a disk or a logical drive.

dd – A UNIX/Linux program that allows you to backup media. You can create a bit-by-bit copy of the original media, one that is forensically equivalent to the original source.

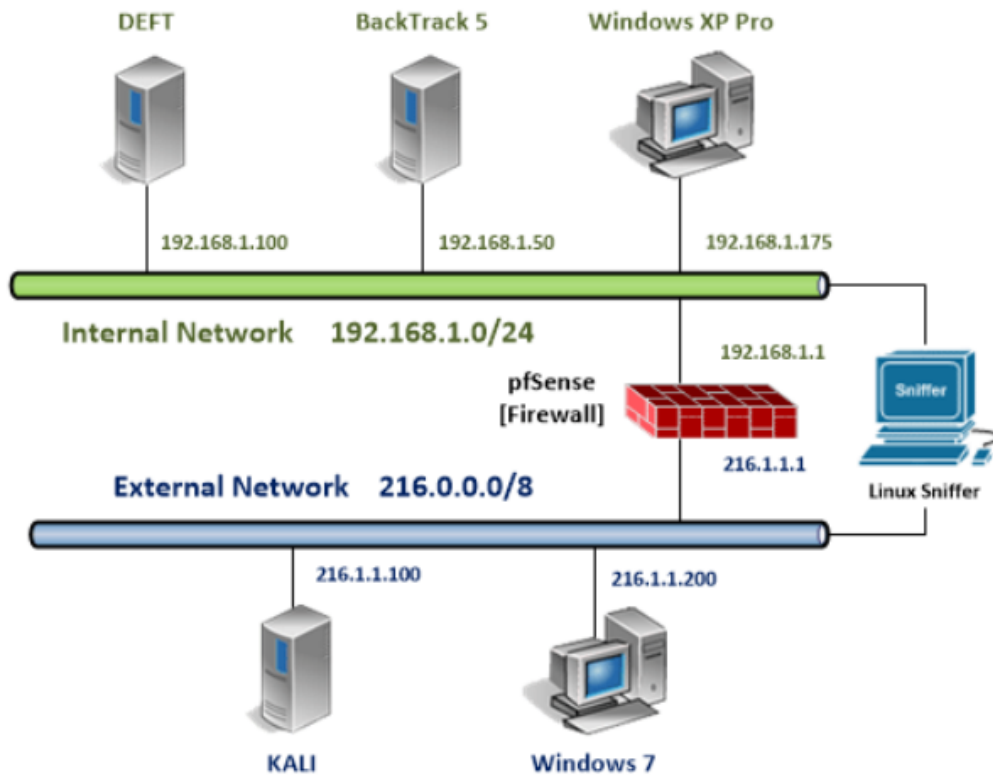
dcfldd – An improved version of the dd program that includes a hashing function.

HELIX– HELIX is a combination of a Live CD and an Incident Response CD. The free version, also known as HELIX 3, is available from e-fense at <http://www.e-fense.com/products.php>. The newest version is based on the Ubuntu CD. When you boot to the HELIX Live CD, it will not automatically mount drives, so disk contamination can be avoided.

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-160, which is 160 bits, are more accurate than the 128 bit MD5.



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 XP Pro Internal Machine | 192.168.1.175 | student | <none> |
| Windows 7 External Machine | 216.1.1.200 | student | password |



1 Using FTK Imager

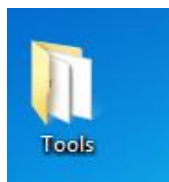
Disks are imaged, or copied, so that an examiner can work on a copy of the disk as opposed to analyzing the actual drive. A disk can be imaged from within Windows using a Graphical User Interface (GUI) based tool like FTK Imager. You can run into complications imaging a disk within Windows because certain files are locked by the OS.

1.1 Imaging a Disk within Windows

1. Login to the **Windows 7 External Machine** by clicking 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.



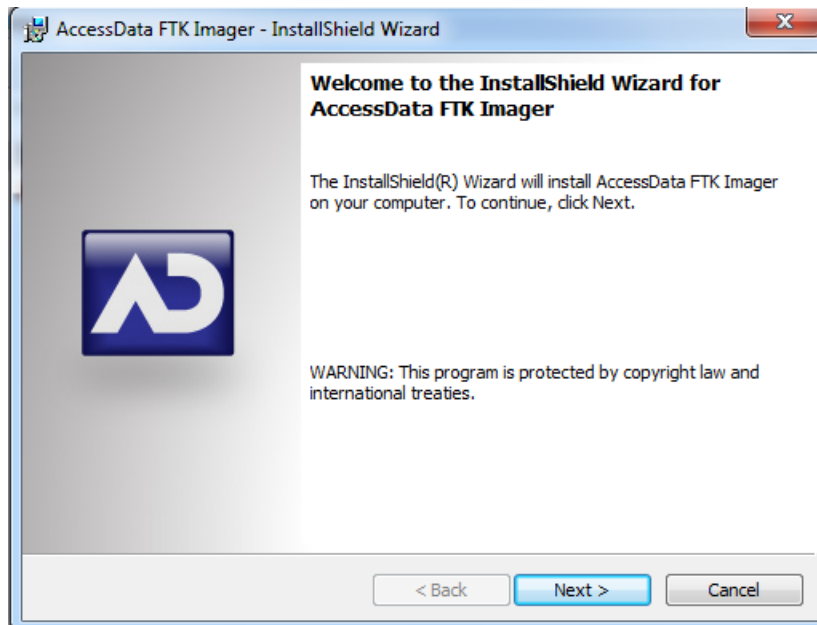
4. Double-click the **Tools** folder on the desktop.



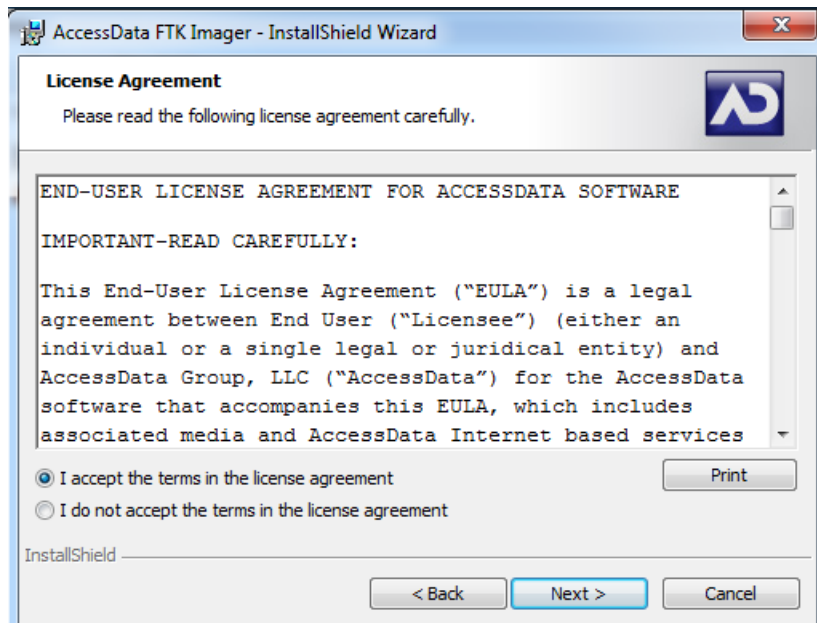
5. Double-click the **AccessData FTK Imager 3.1.3.exe** file.



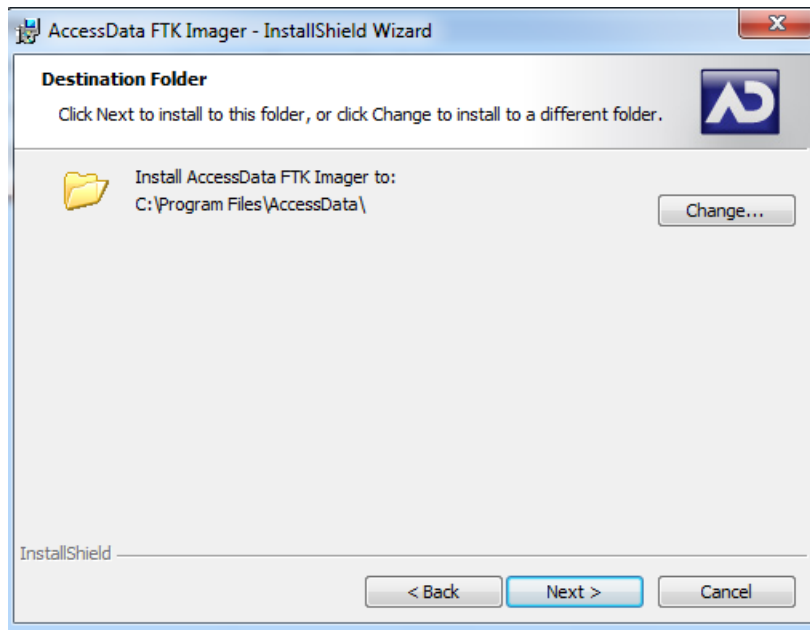
6. Click **Next** at the Welcome to the InstallShield Wizard for AccessData FTK Imager.



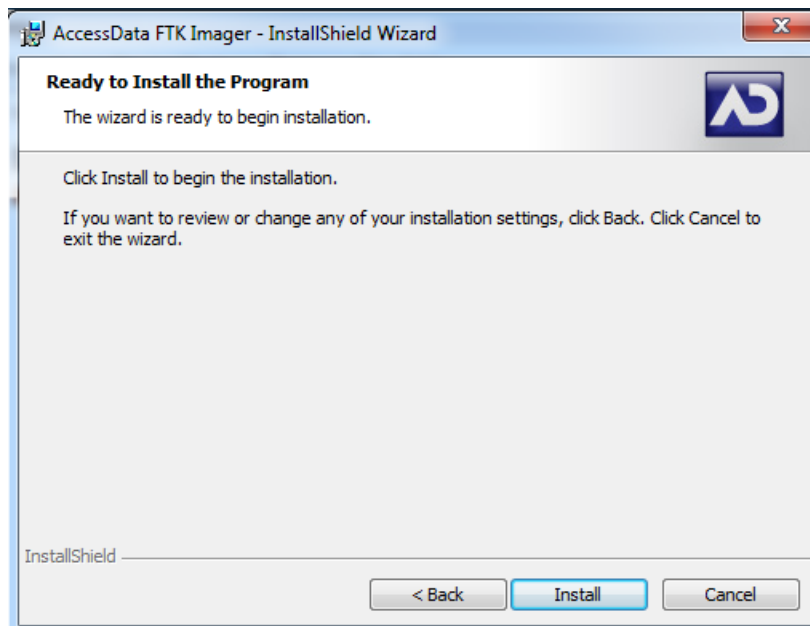
7. Click the **I accept the terms in the license agreement** checkbox and click **Next**.



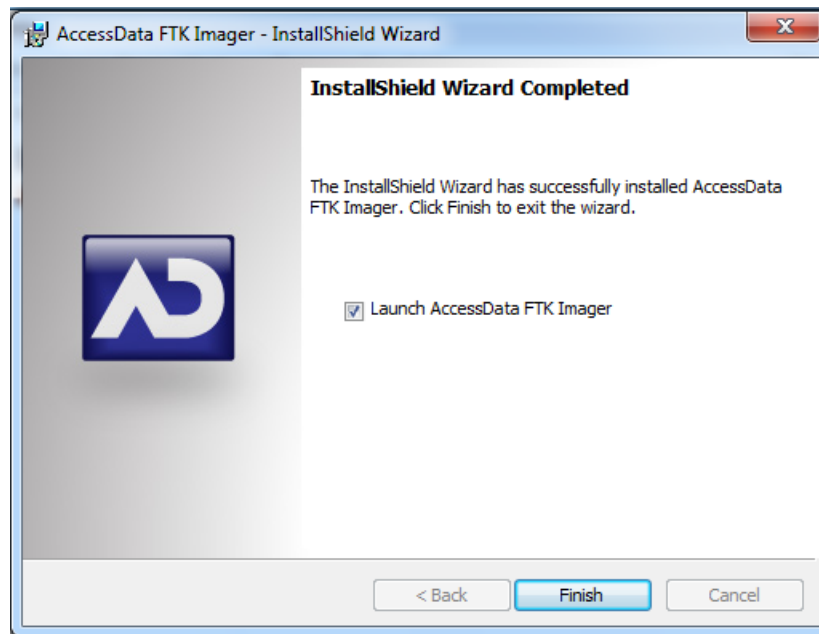
8. Accept the default destination folder and click **Next**.



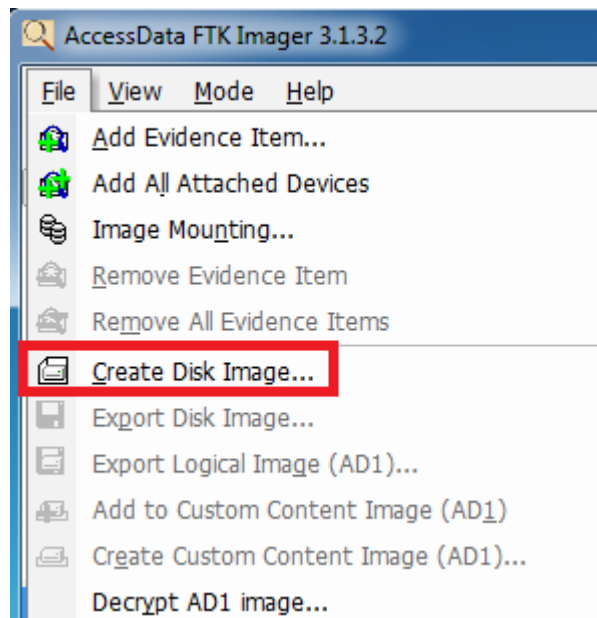
9. Click **Install** to install AccessData FTK Imager.



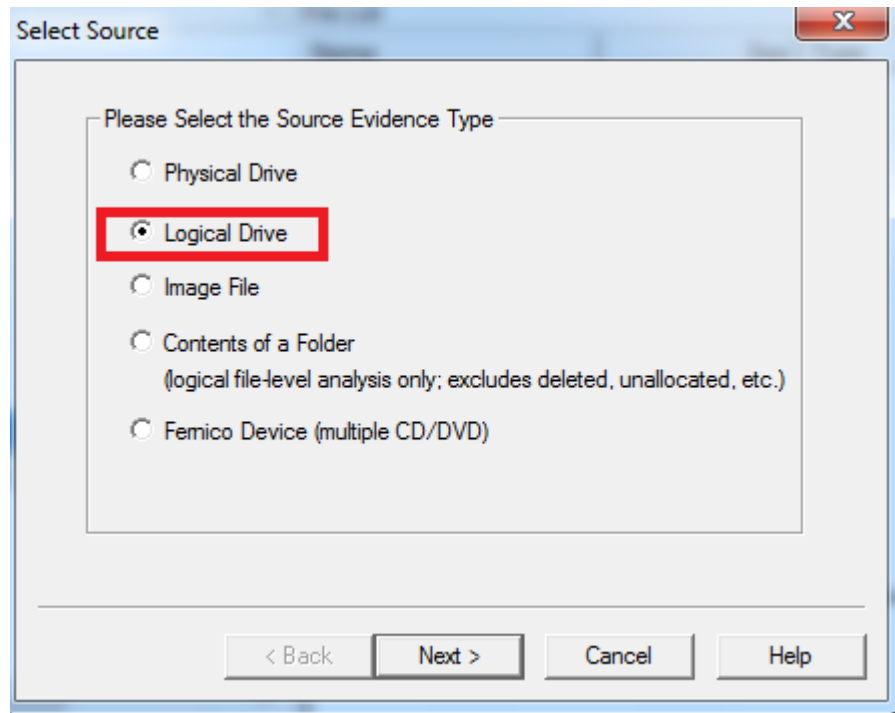
10. Click **Finish** at the InstallShield Wizard Completed screen.



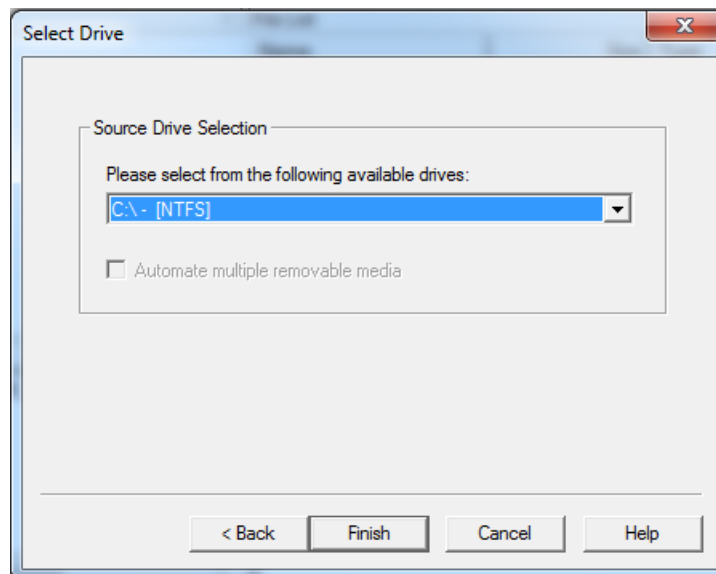
11. In the AccessData window, click **File** in the upper left and select **Create Disk Image** from the drop-down menu.



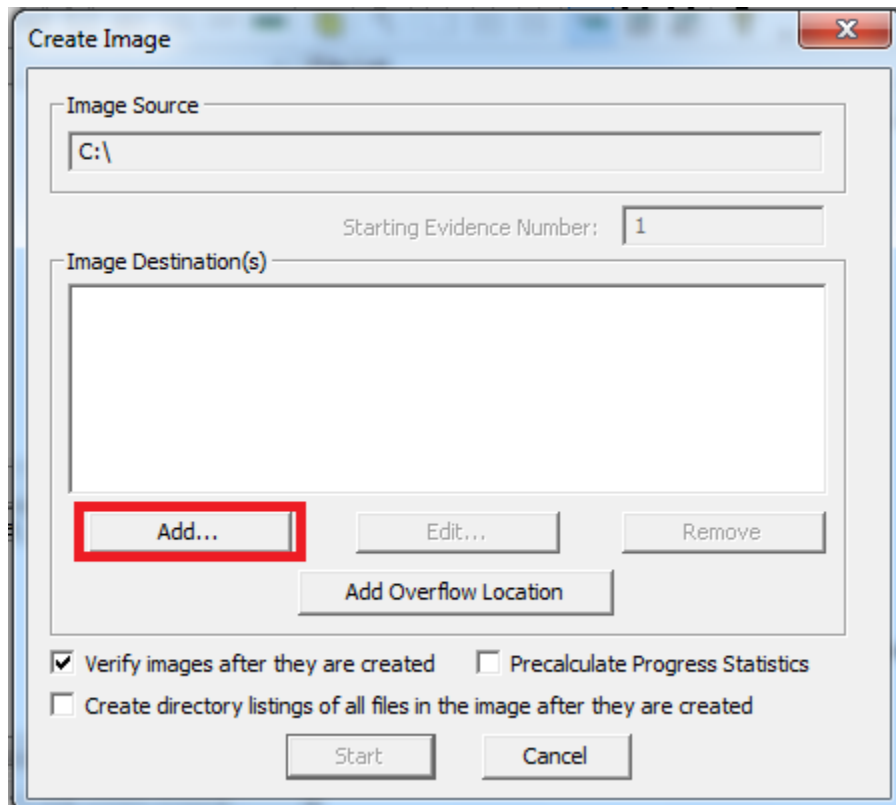
12. At the Select Source screen, select **Logical Drive** for the Source Evidence Type. If a disk is chosen, the entire disk will be copied. If logical drive is selected, a drive letter list will be available from a drop-down box where the user can choose a drive letter. Click **Next**.



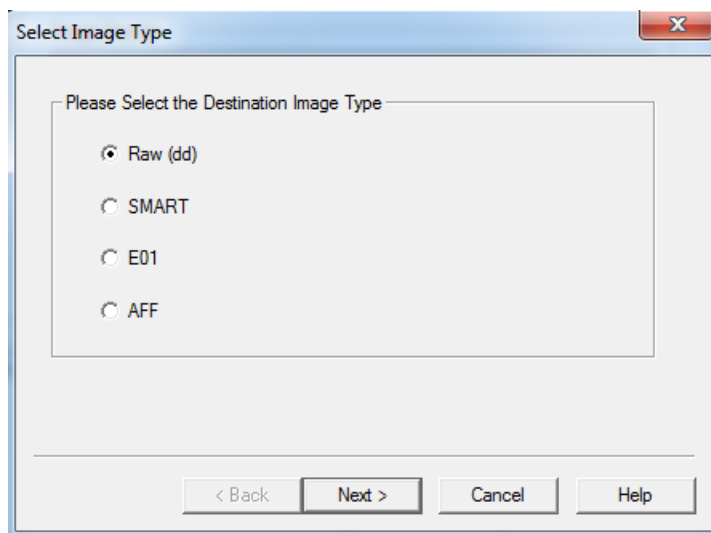
13. Select the C:\ - [NTFS] drive from the Dropdown list and click **Finish**.



14. At the Create Image Screen of FTK Imager, click the **Add** button.

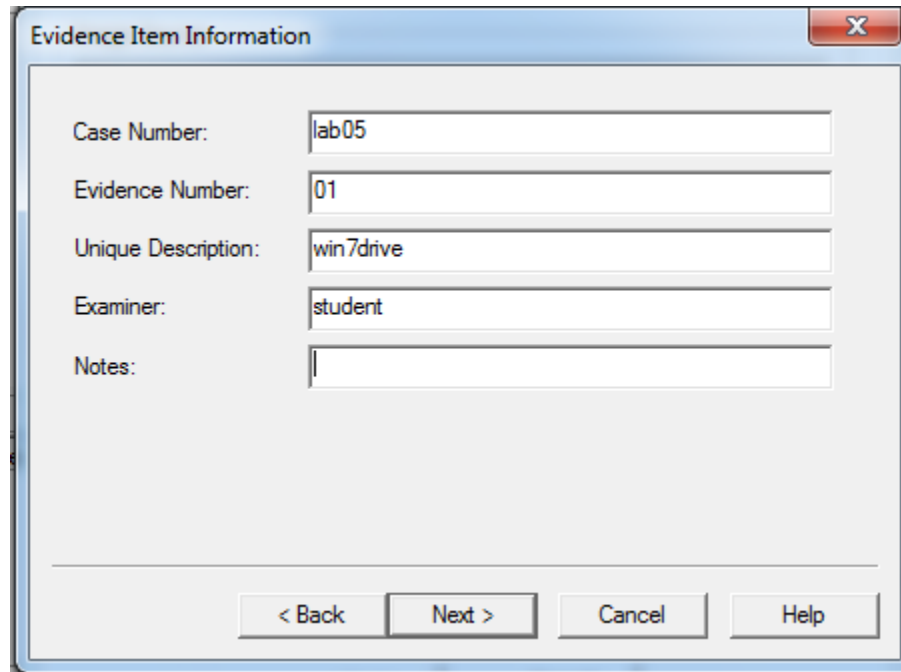


15. Select **Raw (dd)** as the Destination Image Type. Click **Next**.



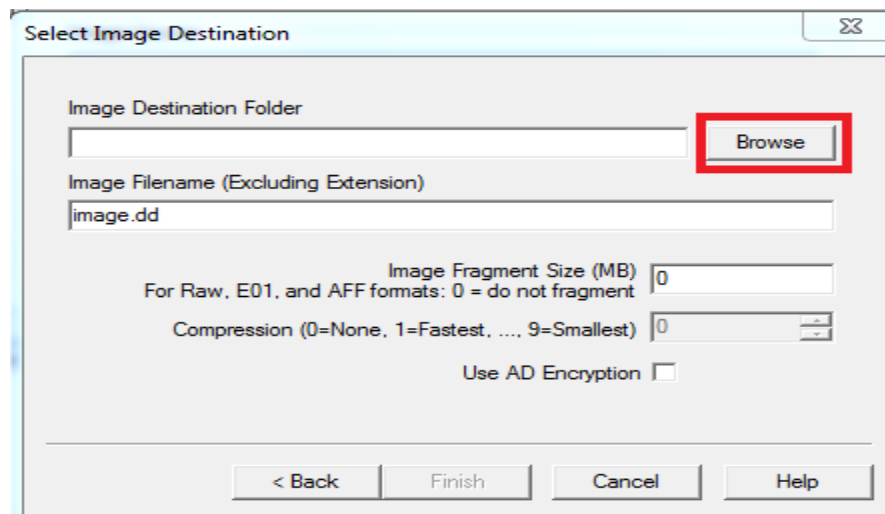
16. Enter the values from the table below into the Evidence Item Information form and click **Next**.

| | |
|---------------------|-------------|
| Case Number: | lab05 |
| Evidence Number: | 01 |
| Unique Description: | Win7drive |
| Examiner: | student |
| Notes: | Leave Blank |



The dialog box titled "Evidence Item Information" contains five text input fields. The first four fields are filled with the values from the table: "lab05", "01", "win7drive", and "student". The fifth field, "Notes", is empty. At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

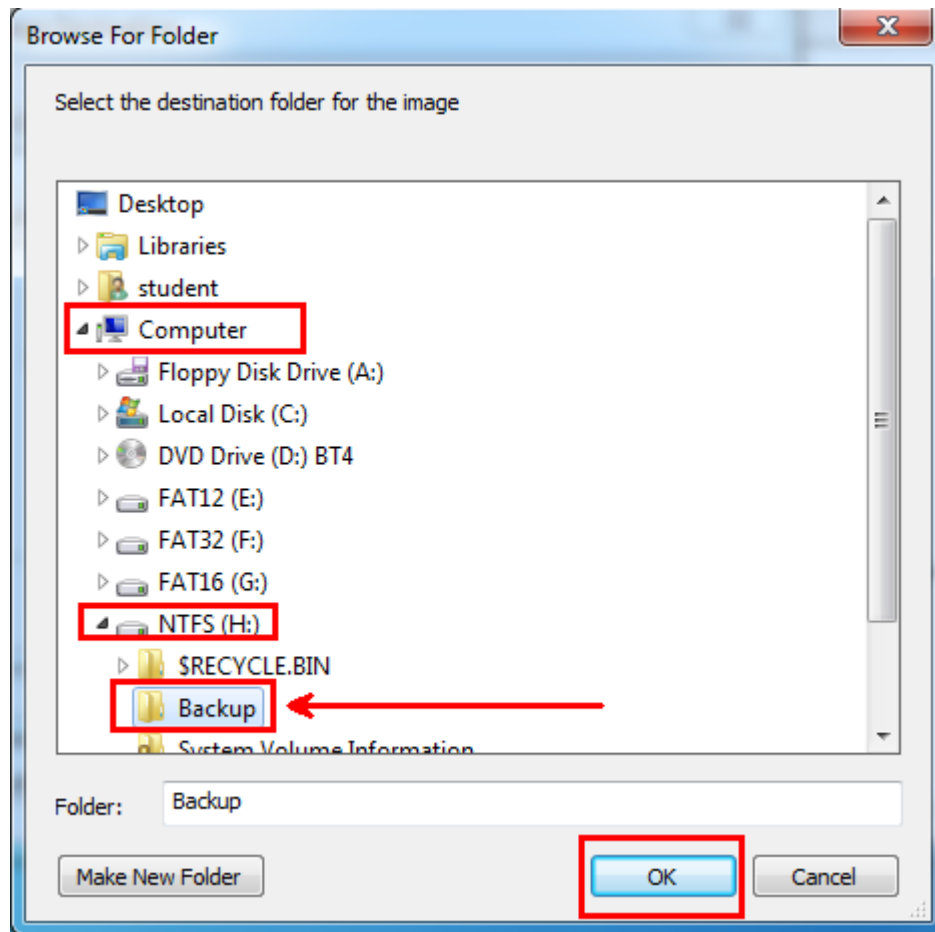
17. Type **image.dd** for the filename and **0** for the Image fragment size. Click **Browse**.



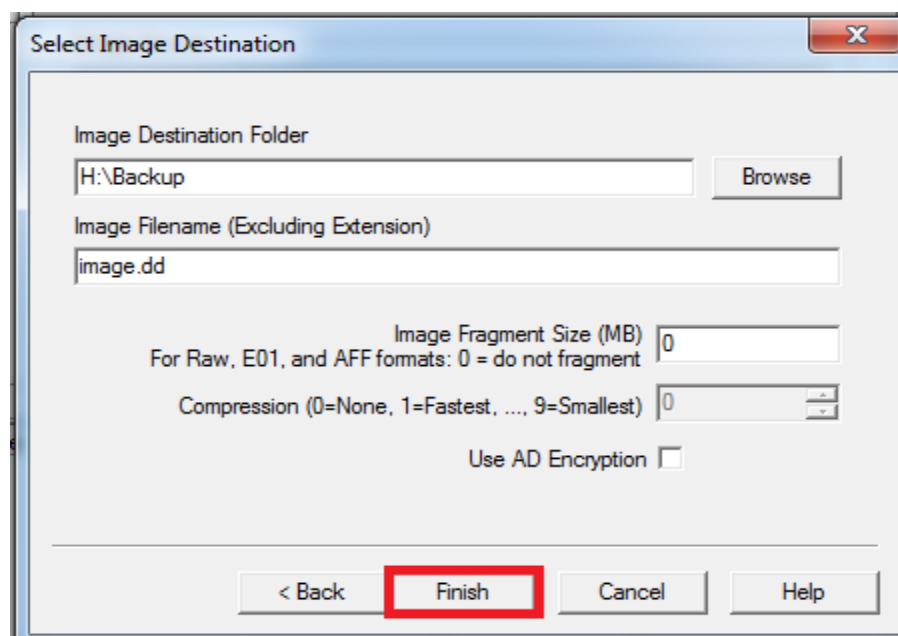
The dialog box titled "Select Image Destination" contains several fields and buttons. The "Image Destination Folder" field is empty, and the "Browse" button next to it is highlighted with a red rectangle. The "Image Filename (Excluding Extension)" field is filled with "image.dd". The "Image Fragment Size (MB)" field is filled with "0". Below it, a note reads "For Raw, E01, and AFF formats: 0 = do not fragment". The "Compression" field is filled with "0". The "Use AD Encryption" checkbox is unchecked. At the bottom, there are four buttons: "< Back", "Finish", "Cancel", and "Help".

NFAT32 has a file limitation of 4 GB files. When imaging disks larger than 4 GB, you will need to change the Image Fragment Size, if your destination disk is FAT32.

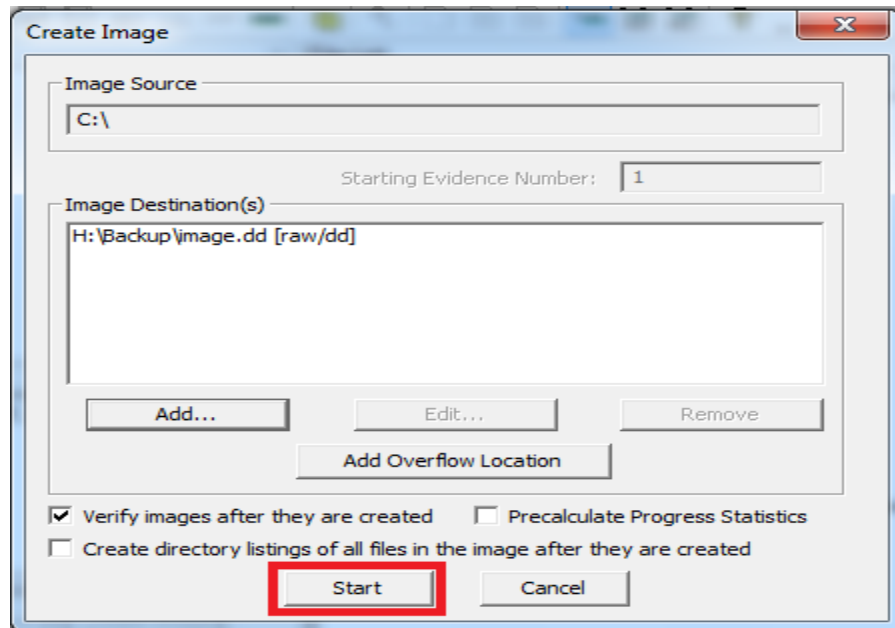
18. In the Browse For Folder window, select **Computer > NTFS (H:) > Backup**. Click **OK**.



19. Click **Finish** to close the Select Image Destination screen.

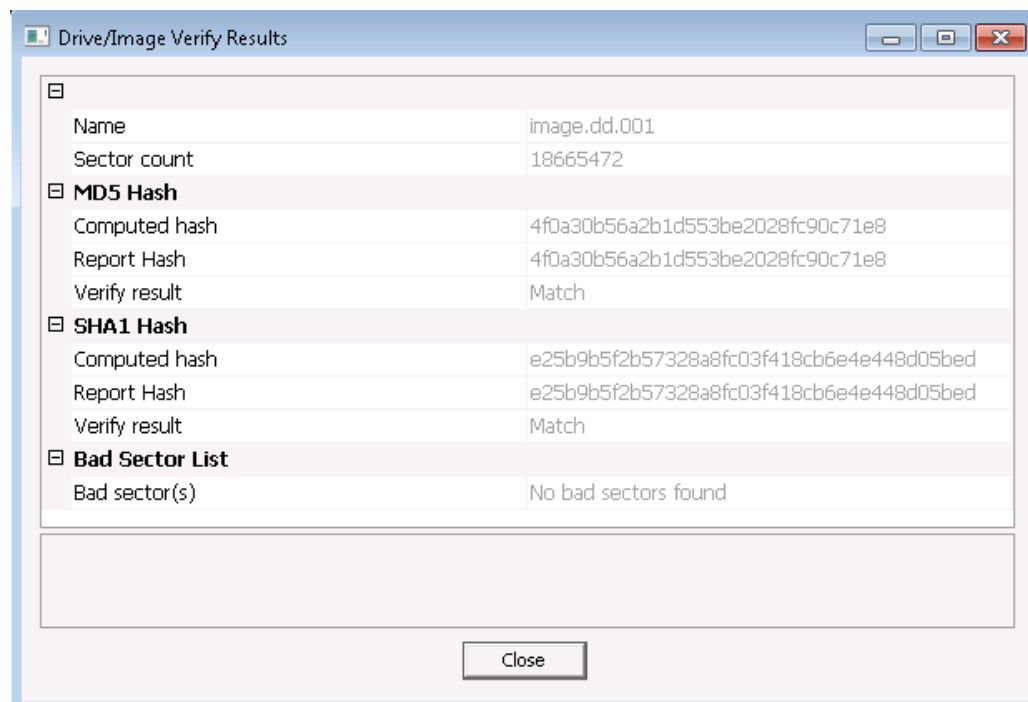


20. Verify that the Image Destination path is set to **H:\Backup\image.dd [raw/dd]**. Click the **Start** button to create the disk image of the logical drive.

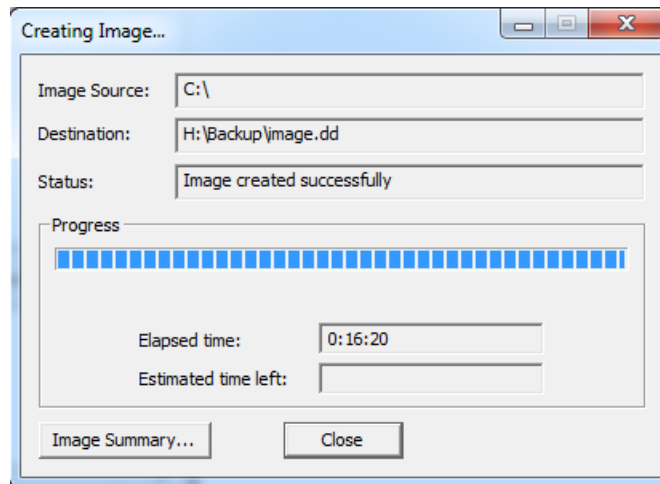


The disk image process can take about 20 minutes to complete. In the real world, logical drives can be several terabytes, and the imaging process can take several hours.

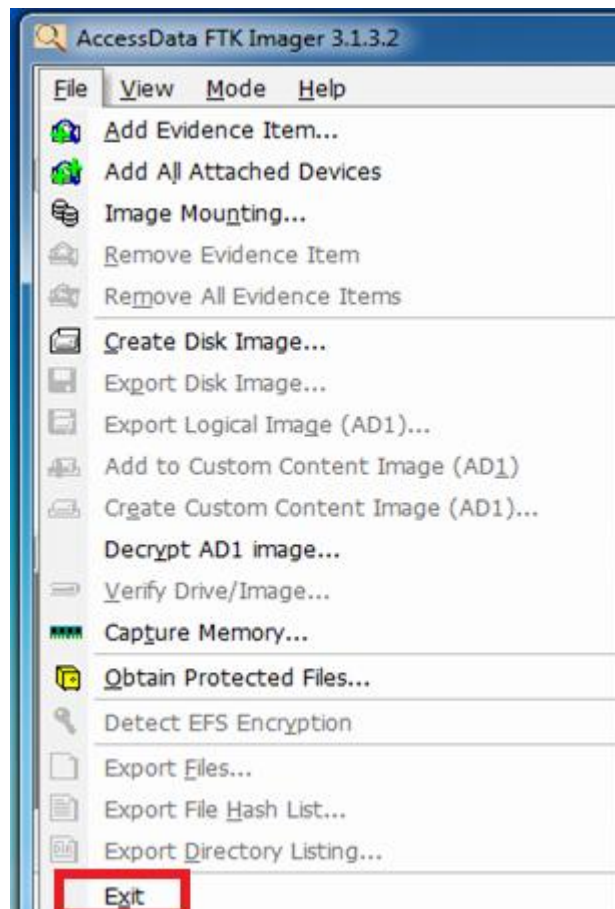
21. All hashes should match. Click **Close** to the Drive/Image Verify Results.



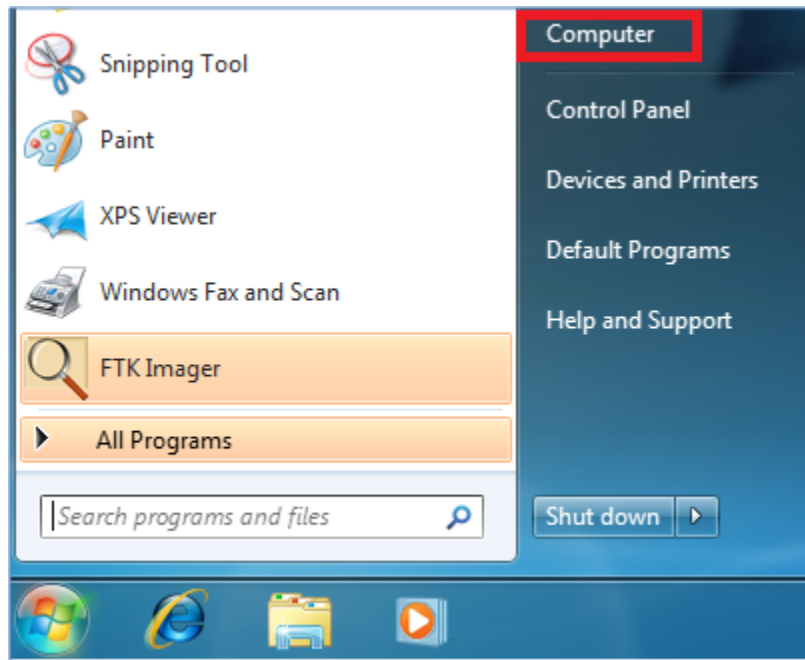
22. Click **Close** to close the Creating Image Screen of Access Data's FTK Imager.



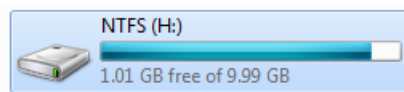
23. Select File from the Menu bar and then select **Exit**.



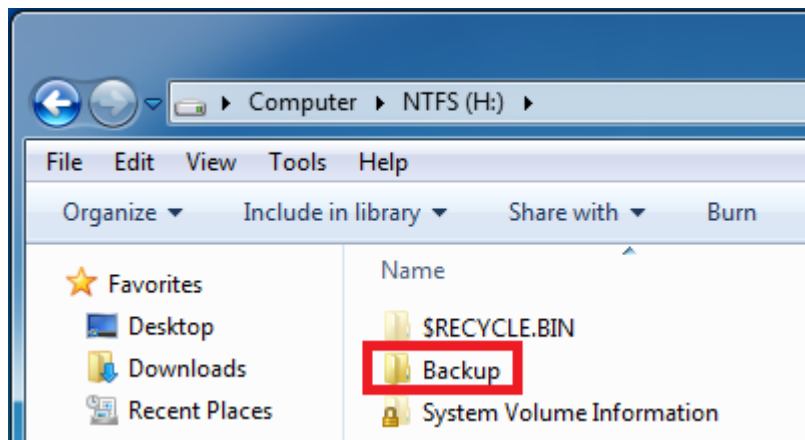
24. Close the Tool Folder. Click on the Start button and select **Computer** from the menu bar.



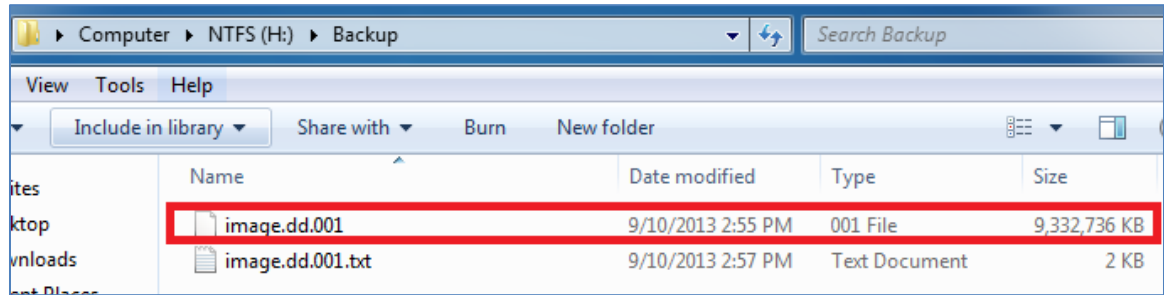
25. Double-click on the **NTFS (H:)** drive where the destination image was sent.



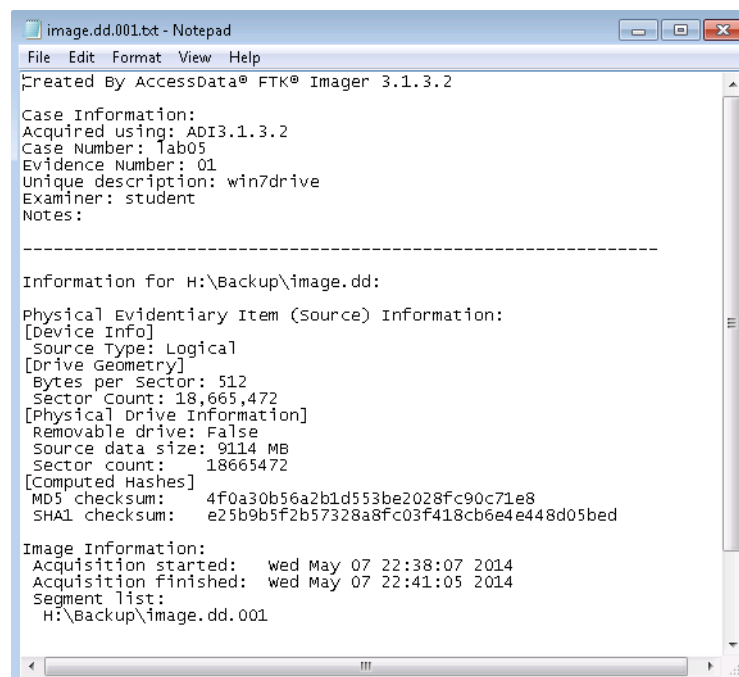
26. Double-click on the **Backup** folder where the image file is stored.



27. Notice that the image.dd.001 image and image.dd.001.txt files are listed. Notice the image.dd.001 file size.



28. Double-click on image.dd.001.txt. View the summary of the image process.



Close all open windows and the Windows 7 PC Viewer.

1.2 Conclusion

FTK 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 within Windows because certain files are locked by the OS. FTK Imager allows you to image a disk or a logical drive.

1.3 Discussion Questions

1. What company makes FTK Imager?
2. Why can issues arise when you image a disk within the Windows OS?
3. What is the largest file that can be stored on a disk with the FAT32 file system?
4. What needs to be done if you image a large drive and the destination disk is FAT32?

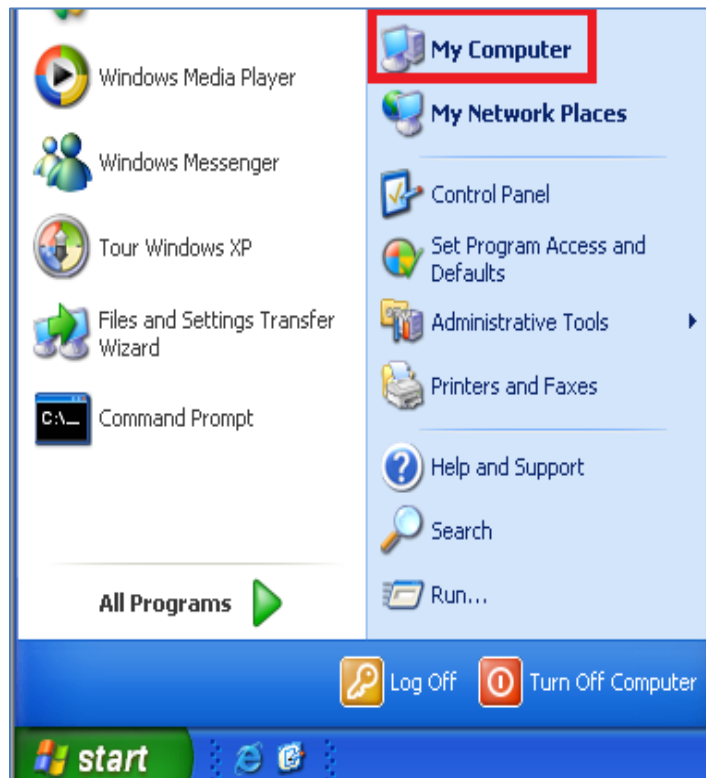


2 Using HELIX to Image a System

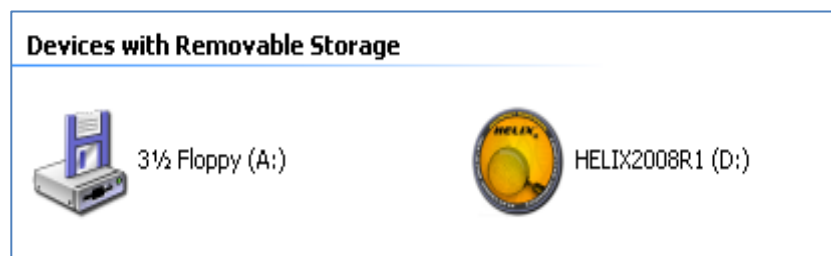
HELIX is a combination of a Live CD and an Incident Response CD. The free version, also known as HELIX 3, is available from e-fense at <http://www.e-fense.com/products.php>. The newest version is based on the Ubuntu CD. When you boot to the HELIX Live CD, it will not automatically mount drives so disk contamination can be avoided.

2.1 Using HELIX

1. Login to the **Windows XP Pro Machine** by clicking on the **Windows XP Pro** icon on the topology.
2. Click on Start and select **My Computer**.



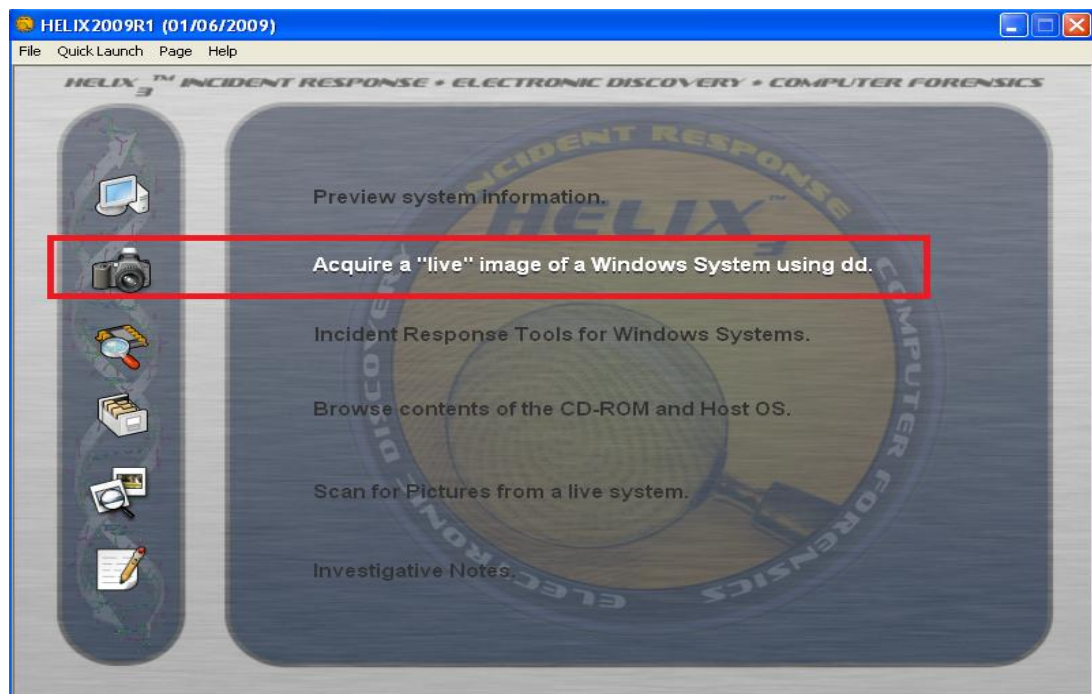
3. Double-click on **HELIX2008R1 (D:)**



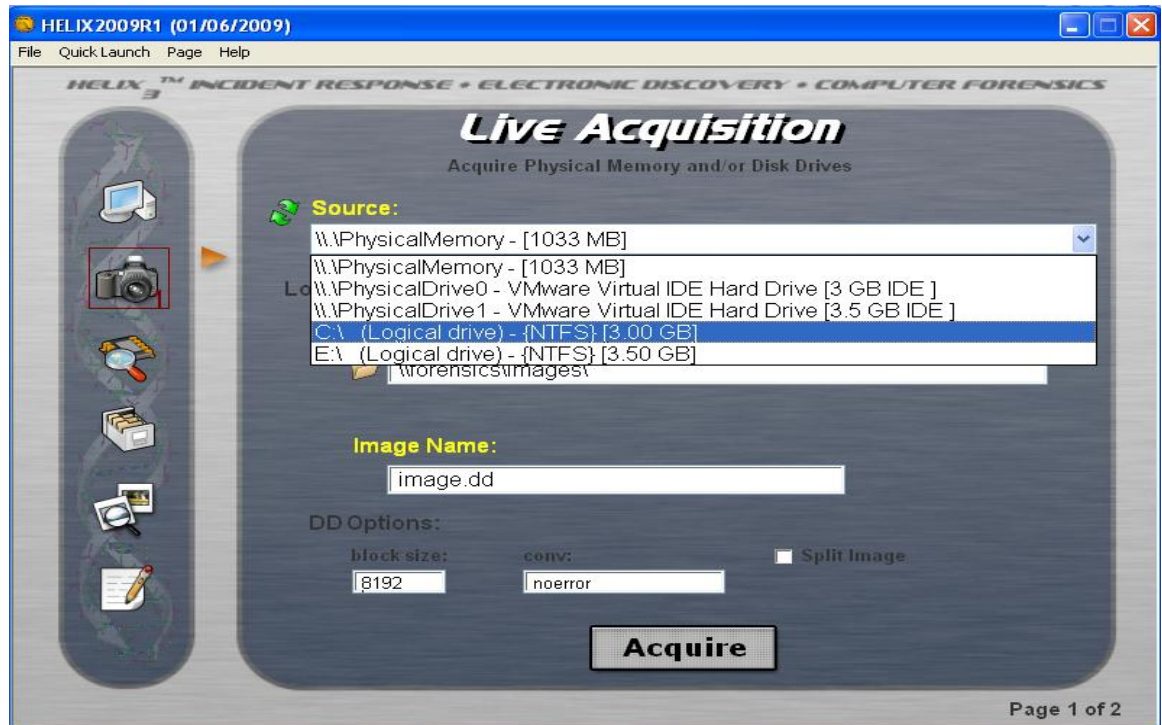
- Click on **Accept** when the HELIX WARNING box pops up on your screen.



- Click the Camera to select **Acquire a "live" image of Windows System using dd.**



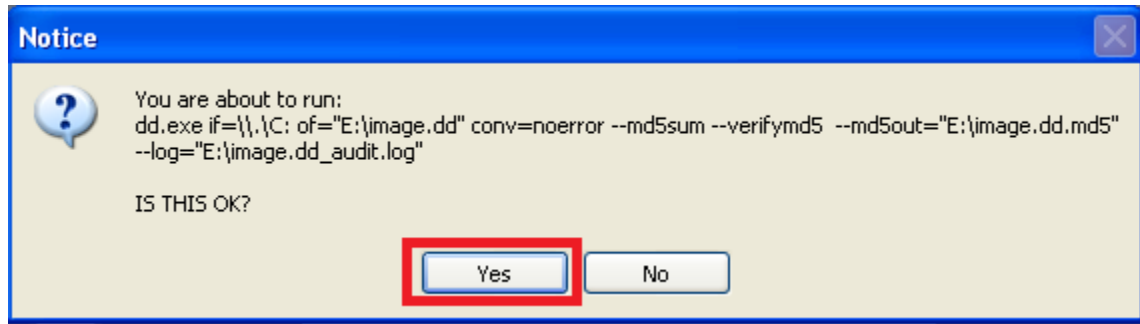
- Click the arrow for the source and select **C:\ (Logical drive) – {NTFS} [3.00 GB]**.



- Change the Destination from the default to **E:** and then click the **Acquire** button.

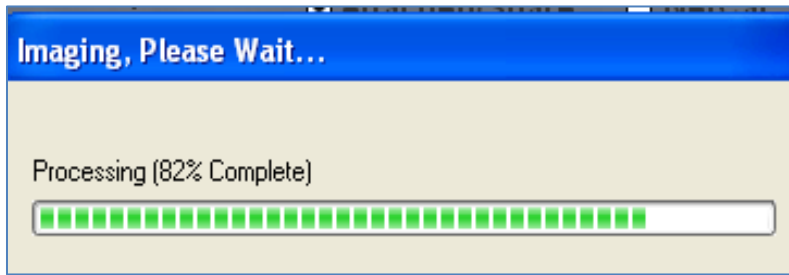


- Click **Yes** to the message box stating that you are about to run the dd command.

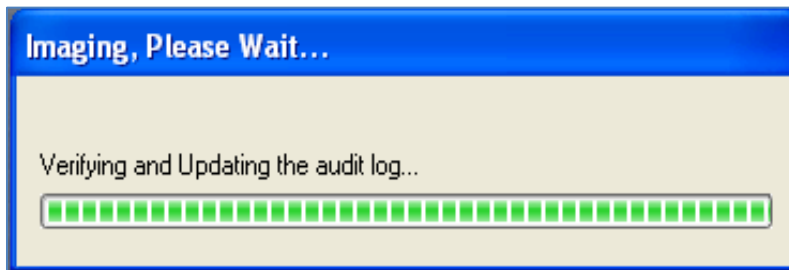


The disk image process will take several minutes to complete. You can move on to the next section and come back when the imaging process has finished.

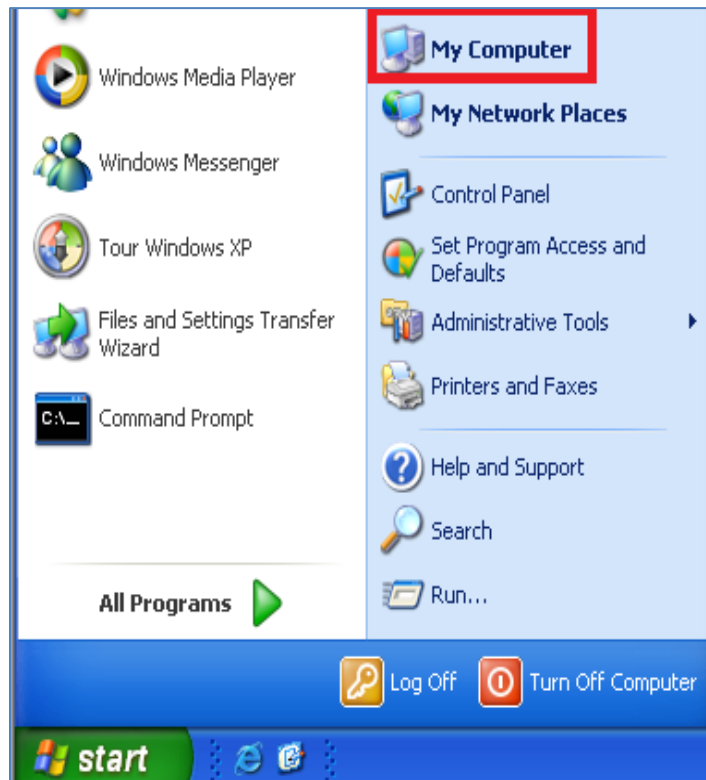
A **Please Wait** screen appears. An image of the logical drive C: is being written to E:



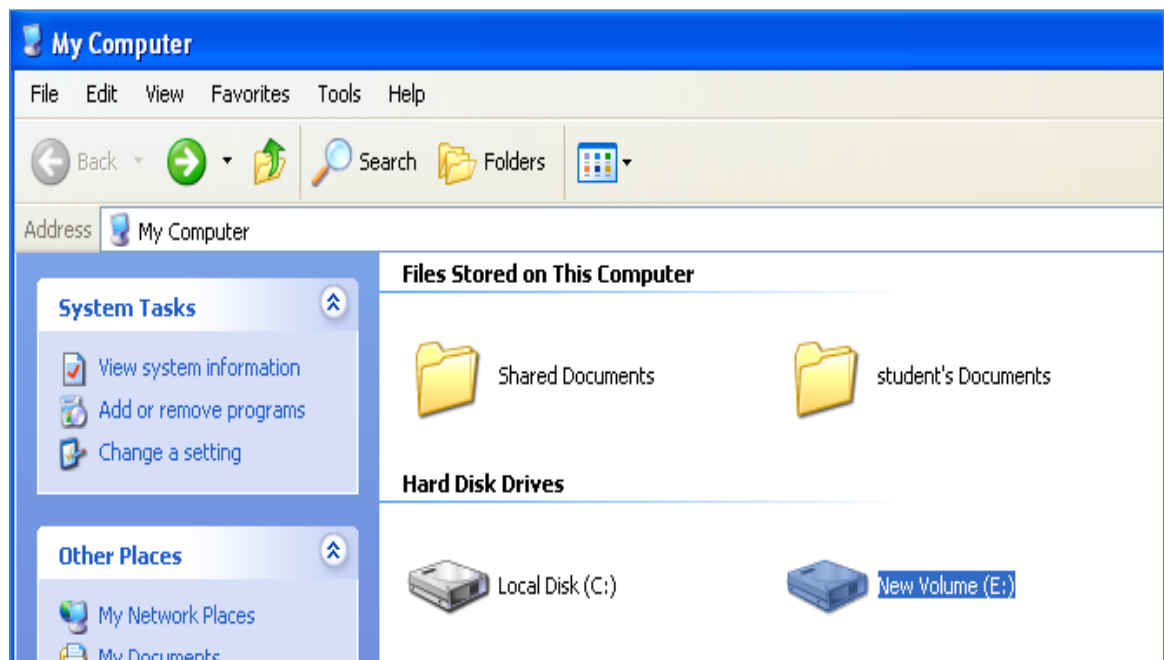
After the image has been created, an audit log and an md5 file will be created.



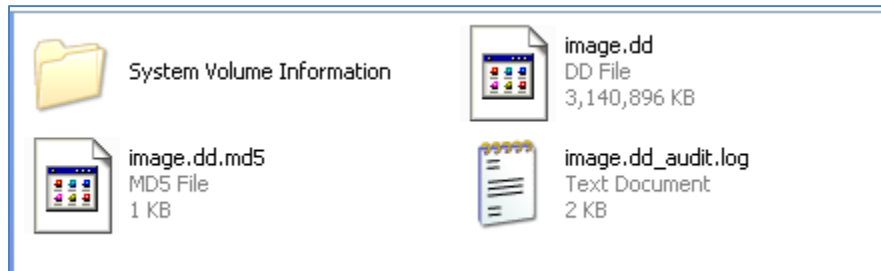
9. On the Windows XP Pro Internal Machine, click on Start and select **My Computer**.



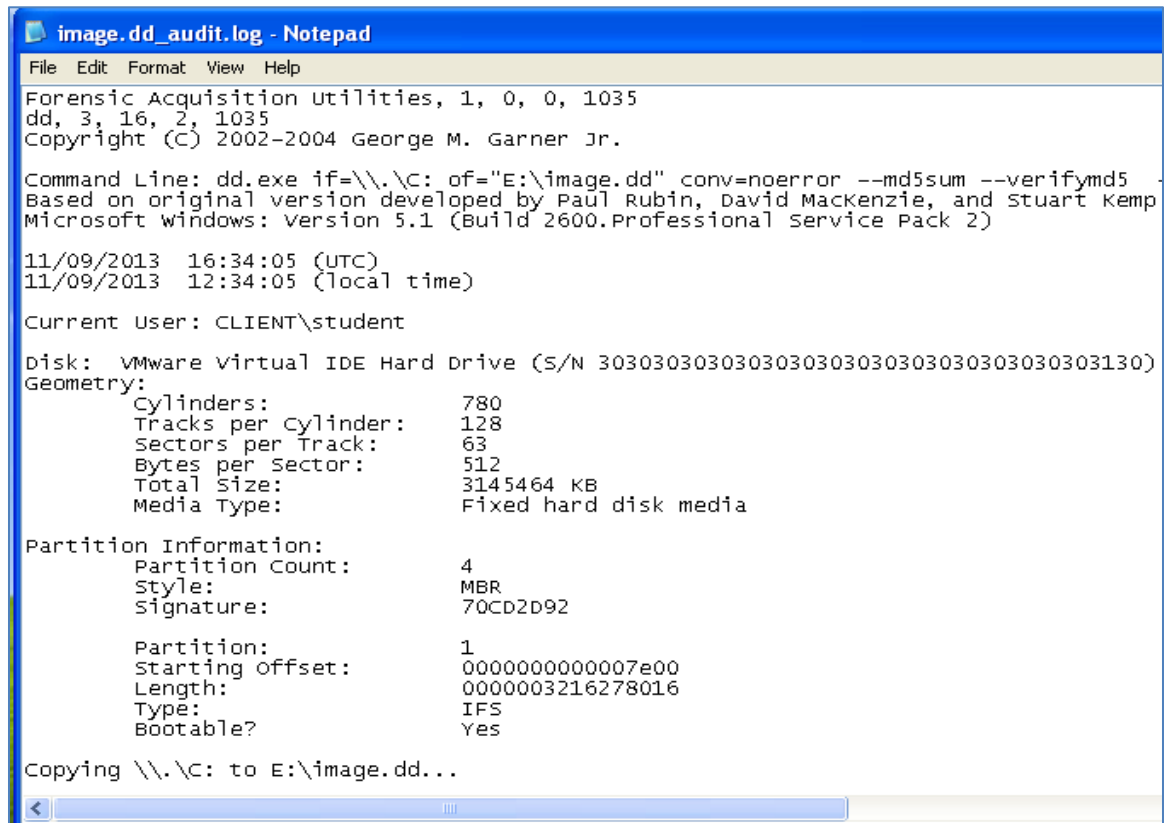
10. Double-click on **New Volume (E:)**, which is the location of the image file.



11. View the 3 files that were created during the imaging process.



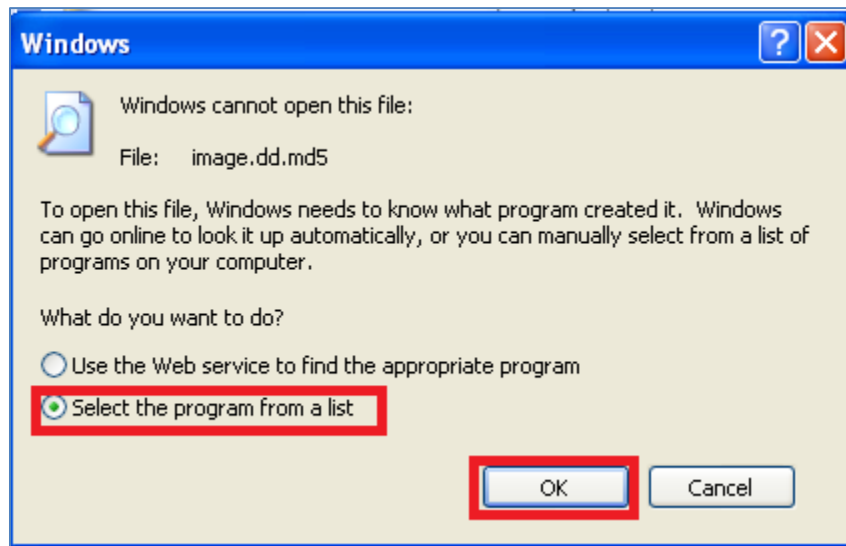
12. Double-click on the **image.dd_audit.log** file to view information about the image.



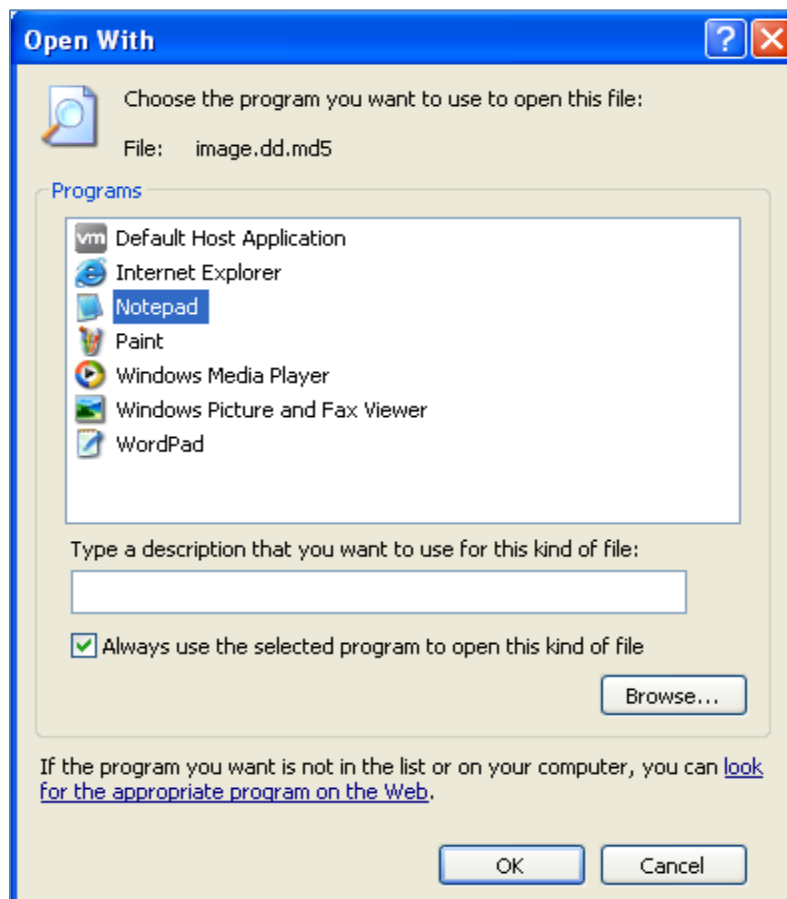
13. Close the audit.log file. Double-click on image.dd.md5.



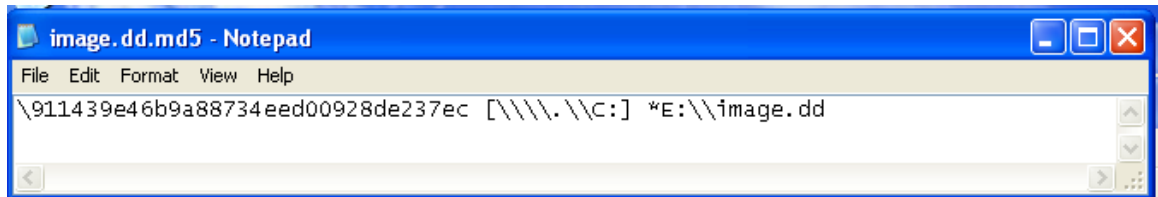
14. Click the radio button for **Select the program from a list** and click **OK**.



15. Click **Notepad** from the list of programs to open the file with (Default). Click **OK**.



16. Close the image.dd.md5 file when you are finished viewing the file.



17. Close the Helix application and select **No** when asked if you want to save a PD log file of all your actions. Close all open windows and the Windows XP Pro PC Viewer.

2.2 Conclusion

HELIX is a Live CD/DVD, which has incident response functions as well as imaging capabilities. HELIX from e-fense, is based on Ubuntu, and is available for download as HELIX 3 at <http://www.e-fense.com/products.php>. If HELIX is used to create an image within Microsoft Windows, an image file, audit log, and MD5 hash file will all be created.

2.3 Discussion Questions

1. What is the name of the free version of HELIX?
2. The newest versions of HELIX are based on what Linux Distribution?
3. What three files are created when HELIX is used to image a drive?
4. HELIX provides what hashing algorithm after completing the imaging process?

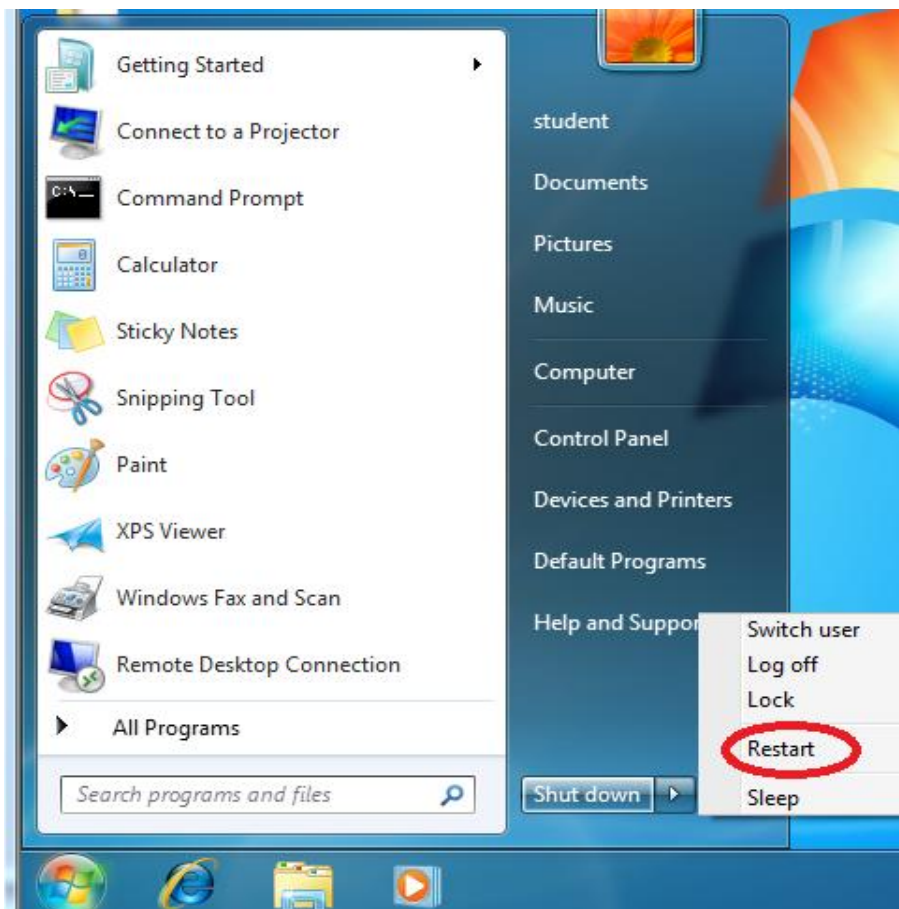
3 Using BackTrack to Image a System

In the first two exercises, we used GUI tools to image a drive while Windows was running. It does not always work well to image a disk while the operating system is up and running because certain files are locked by the Windows operating system. However, if disk encryption is being utilized, it is best to image the device while the operating system is up and running. In cases where disk encryption is not being utilized, it may be best to shut the system down completely and image the system's disk.

3.1 Booting to the Live DVD Environment

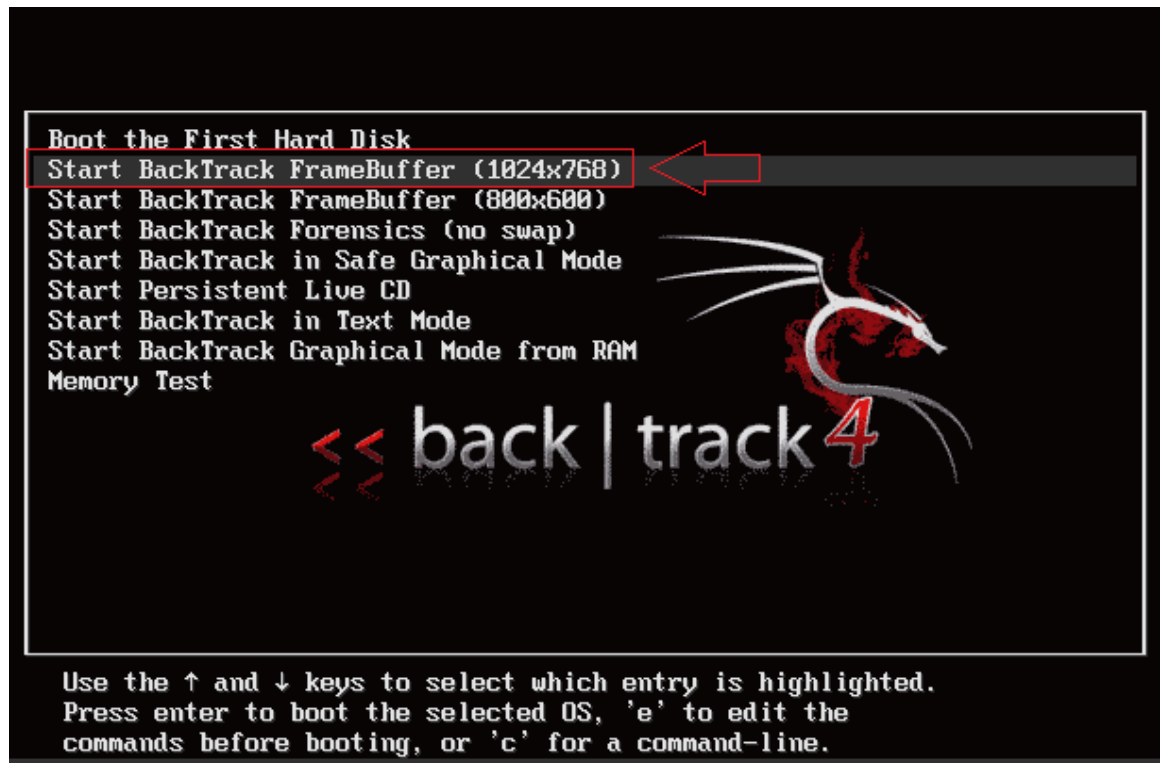
Perform the following steps on the Windows 7 External Machine.

1. Click Start, click the arrow to the right of Shut down and click **Restart**.



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

2. Choose the second choice shown in the Boot Menu.



3. Type the following command to initialize the Graphical User Interface (GUI):
`root@bt:~# startx`

```
BackTrack 4 R2 (CodeName Nemesis) Security Auditing
For more information visit: http://www.backtrack-linux.org/
root@bt:~# startx
```

4. 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.



5. 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
```

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

6. 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. The partition will be mounted as read-only by adding the ro option to the mount command.

7. Type the following command to mount the NTFS partition:

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

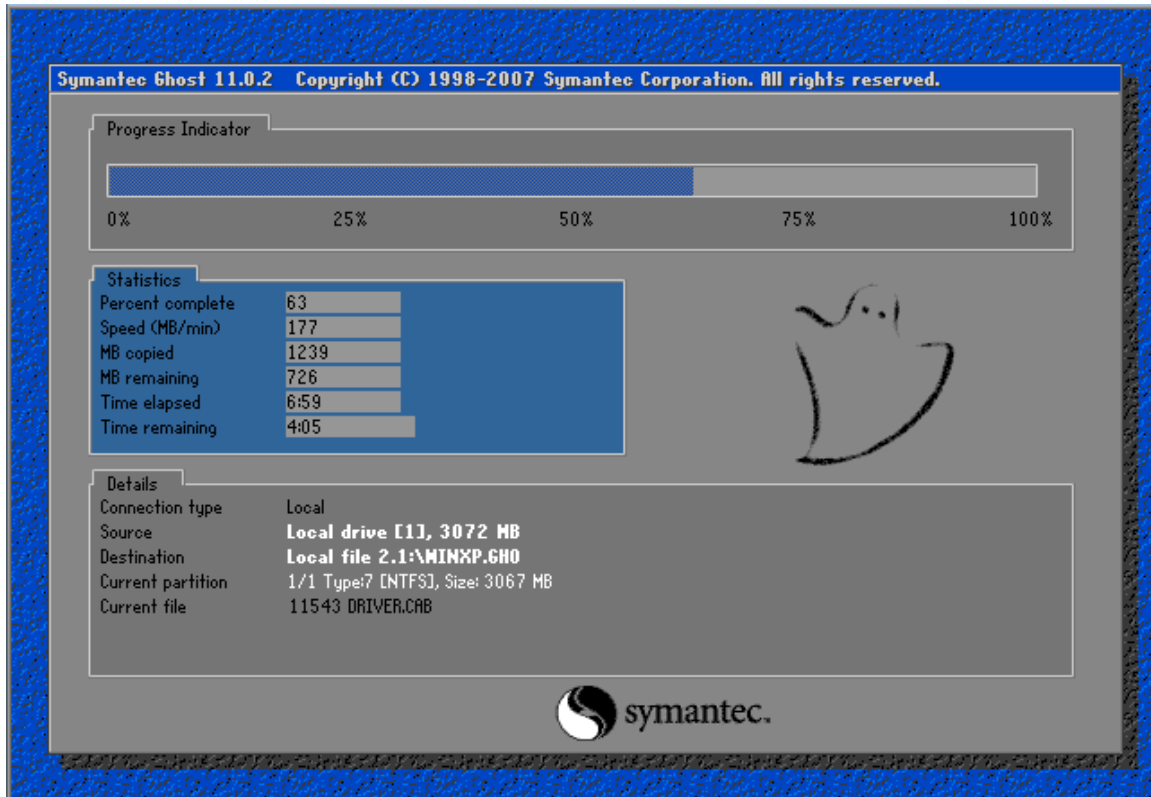
```
root@bt:~# ntfs-3g /dev/sdd1 /mnt/sdd1
```

8. 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)
```

The Linux/Unix program `dd` will allow you to make a backup copy of media. Many network administrators are familiar with the program Norton Ghost. This commercial product from Symantec, which is widely used in the industry, is used to back up all of a drive's data, including the operating system. The `dd` program is open source and allows you to make an exact (bit-by-bit) copy of your original media. This will include all of the deleted files and folders, as well as any slack space that existed on this disk.



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.

- To make a copy of the second SATA drive using `dd`, type the following:
`root@bt:~# dd if=/dev/sdb of=/mnt/sdd1/satadrive2img.dd`

```
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
```

This time we make a forensic copy of the disk, not just the partition (logical drive).

The `dcfldd` command is an enhanced version of `dd` that provides status updates and allows the user to have the hash value of the image calculated during imaging.

10. To make a copy of the third SATA drive using `dcfldd`, type the following:

```
root@bt:~# dcfldd if=/dev/sdc of=/mnt/sdd1/satadrive2img.dd
```

```
root@bt:~# dcfldd if=/dev/sdc of=/mnt/sdd1/satadrive2img.dd
3072 blocks (96Mb) written.
3264+0 records in
3264+0 records out
```

Close all open windows and the Windows 7 PC Viewer.

3.2 Conclusion

While imaging disks is possible within the Microsoft Windows operating system with a GUI tool such as FTK Imager or HELIX, it is not always advised because certain operating system files are locked. However, if a disk is using encryption, you do not want to shut it down and take an image. If disk encryption is not in use, you may want to shut the system down and image it with a Linux Live CD/DVD like BackTrack or HELIX.

3.3 Discussion Questions

1. What is a Live CD/DVD?
2. What is Norton Ghost?
3. What does the `dd` command allow you to do?
4. What is the difference between using `dd` and the `dcfldd` command?

References

1. HELIX 3:
<http://www.e-fense.com/products.php>
2. FTK Imager:
<http://www.accessdata.com/support/product-downloads>
3. The dd Command:
<http://www.computerhope.com/unix/dd.htm>
4. The dcfldd Command:
<http://dcfldd.sourceforge.net/>
5. MD5 Hash Explained:
<http://www.makeuseof.com/tag/md5-hash-stuff-means-technology-explained/>

