Acquiring and Validating Digital Evidence

In this information age, digitized data is everywhere you turn. Businesses thrive on the ability to quickly process this data into information to use as a competitive business advantage. Unfortunately, it may be disastrous for a company if sensitive data or information falls in the hands of a competitor. A disgruntled (or greedy) employee may attempt to copy sensitive data and redistribute it to competitors. A digital forensics investigation and analysis may not prevent this from happening, but is part of a proper business response to this type of situation.

For this exercise, you will use the Encase software and hardware write blockers to image a hard drive and verify the digital evidence. This is generally considered the first step in any forensics investigation. If any illegal activity is suspected, it would be best to inform law enforcement and involve them in the process.

The forensics lab is in Jacobs 323. Swipe your UB card at the entrance to gain access to the lab.

Removing the hard drive from the suspect's PC

Your first step is to get your hands on the physical hard drive (or drives) that you want to image and analyze. The suspect PC is labeled **Crash Machine** and is on the table opposite the Forensic Workstations. There is a toolkit with screwdrivers on the table as well. **Do NOT power the suspect's PC on!** Booting a computer will change many files on the hard drive which will compromise your investigation. A savvy employee may even have some sabotage code that runs when the PC is not booted in a particular fashion. This sabotage code may delete important evidence for your investigation.

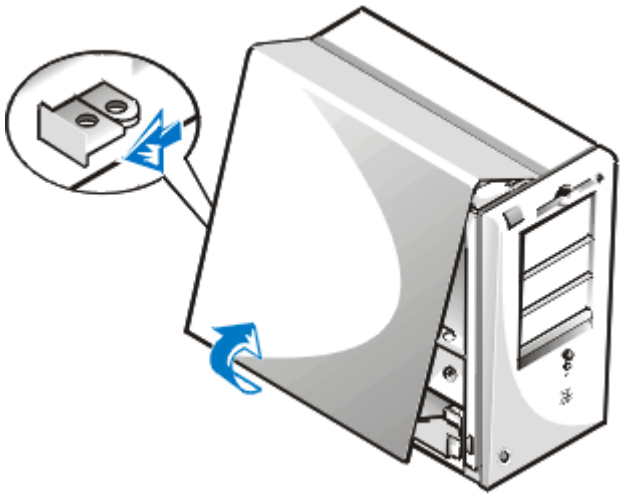
Although you don't need to do this for the lab, it is usually a good idea to take pictures of the desk and surrounding area in order to 1) document your findings and 2) restore the work area back to its original state when you're done. These preliminary investigations usually happen without the employee knowing, so making sure everything is put back in its place will help prevent the employee from being tipped off that they're being investigated.

Before handling any electronic equipment, it should be unplugged and you should take care to ground yourself to limit the transfer of static electricity. To remove the hard drive, you first must remove the outer case of the computer. Each PC will have a different mechanism for removing the case. Some are easy and some not so easy to remove. For this particular Dell machine, one half of the case can be removed to access the internal components of the computer.

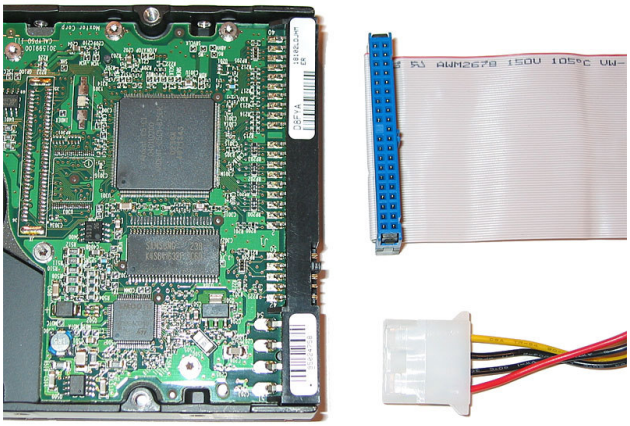
First, in the back of the PC towards the bottom, locate the metal locking mechanism. The arrow on the picture below shows where the locking mechanism is. Next, slide the metal locking mechanism towards the center of the PC so that the two rings are not

lined up. This will disengage part of the locking mechanism that holds the case on. In the picture, it should be moved to the left as far as possible.

Next, press the small plastic button on the front of the case at the bottom to release the one side of the PC case. The arrow in the above picture shows where the button is on the front of the PC. The case can be lifted up and then removed. Here is a visual from Dell's website which illustrates how the case is removed.



Now that the case is removed, you can locate the hard drive (or hard drives) for removal. If you've never seen a hard drive, there is a picture of one on the left below. The image on the right shows the underside of a hard drive, and the locations where the IDE ribbon cable (top) and power cable (bottom) connect to the drive.



Each PC hard drive will have a hard drive ribbon cable and a power cable connected to it. Sometimes, multiples devices (CD ROMs, DVD ROMs, etc) will be daisy chained on a single drive and/or power cable. For this exercise, there is only one hard drive in the PC that you must acquire.

To remove the metal chassis that holds the hard drive, look for a sticker of a green arrow pointing to a single screw. Once you remove that single screw, the entire metal chassis that holds the hard drive can now rotate out towards you. At this point, you will need to disconnect the IDE drive cable and the power cable from the drive. Once the hard drive chassis is rotated out 90 degrees towards you, you can then slide the entire chassis unit up and out. To save some time, I don't recommend removing the hard drive from the chassis since you can image the drive even though it's still attached to the metal chassis.

Record the make, model, capacity and other relevant information about the hard drive you just removed.

_____

_____

_____

Connecting the write blockers

The hardware write blockers are used to prevent any data from being written to the suspect's hard drive during the imaging (copying) process. The specific write blocker cables, power supplies and bridge are already set out on the forensics bench for you. Login to the Encase forensics machine (on the right) with the username **forensics** and password **mgtMSS100**.

Connect the FireWire 800 IDE Bridge to the Hard Drive ensuing that the drive pins line up. Next, connect the firewire cable from FireWire 800 IDE Bridge to firewire port in the front panel of the Alienware PC. The firewire port is next to 2 USB ports on the front of the PC. You may need an adapter for the firewire cable.

Connect the power cable to the FireWire 800 IDE Bridge, Hard Drive and Forensic Computers Drive Power Switch. Make sure the switch is in the Off position.

Connect the power adapter cord from the Forensic Computers Drive Power Switch to the Tableau Power Adapter. Plug the Tableau Power Adapter into the power strip under the table.

Switch the Forensic Computers Drive Power Switch to the On position. You will hear the hard drive begin to make a whirring noise as it powers up. The PC should now recognize another device (drive) attached to the computer.

Open My Computer to browse for the attached devices. The write-blocked hard drive will be listed under the Hard Disk Drives section. Double click the drive letter to browse through the files stored on the drive. Attempt to rename a file on that hard drive write down the message that appears. Also, take note of the drive letter.

_____

_____

Imaging and verifying (hashing) the hard drive image

Start the EnCase program by double clicking on the EnCase icon on the desktop.

Click File, New and enter your new Case information. Change the Name to your name or group. Change the Examiner Name to your name. Click **Finish**.

Click the **Add Device** button on the Toolbar. Select Local Drives on the right pane and click **Next**. Select the drive letter (possibly G:) of the added hard drive and click **Next**.

Is the Write Blocked option selected? Why or why not?

_____

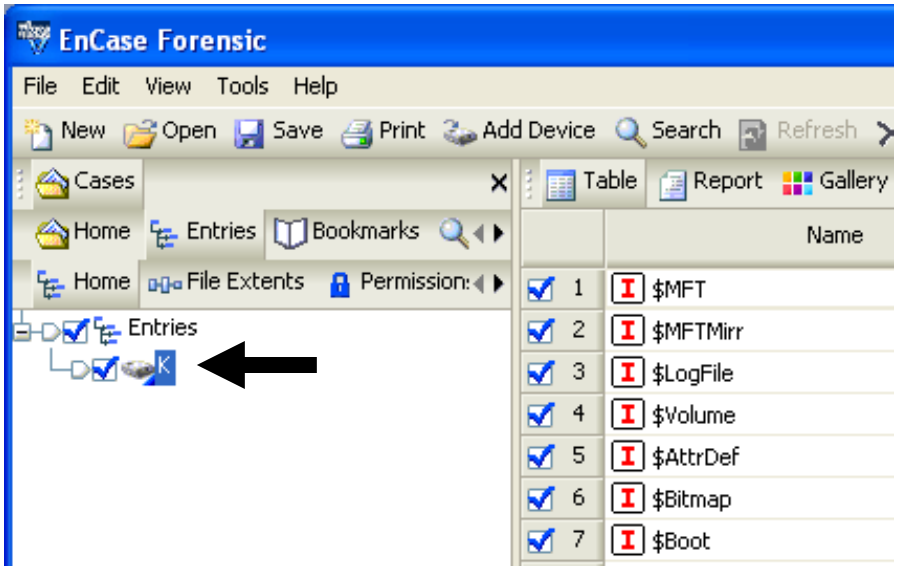
_____

_____

Click **Finish**.

Click on the **View** Menu and make sure the **Auto Fit** option is checked.

Click the check box next to the drive letter of the acquired drive in the tree pane (see arrow below).



An **Acquire** button should now appear on the toolbar. Click on this button to begin the imaging process.

Click **Next**. Enter a name for the evidence. Select **None** for Compression. Click **Finish**.

You will see a flashing message "Acquiring Evidence" and a countdown timer in the bottom right hand corner. This process will take about 10 minutes. While you're waiting for the drive partition to image, you can research and answer the questions on the following page. The only PC with internet connectivity is the Forensics Research Workstation on the left hand side of the Forensics room when you enter.

Additional Questions

1) Aside from MD5, what other hashing algorithms can be used to verify digital evidence?

2) Would it be useful for a digital forensic investigator to use multiple hashing algorithms to verify the digital evidence?

3) For this exercise, you were required to image an IDE hard drive. Identify two other hard drive technologies commonly used today. Hint: Check the write blockers in the tackle box on top of the filing cabinet to see what other hardware write blockers exist.

4) Research and identify an open source drive imaging program.

5) Why don't the primary forensic workstations have Internet connectivity?

By now that the hard drive should be imaged and you should record the results of the Acquire process. The results should include the status, start and stop time, total time, name, path, GUID and Acquisition Hash value. You can easily copy and paste the results from that screen.

_____

_____

Next, you should hash the entire drive to get a unique hash value. To do this, Right click on the drive letter (or evidence name) in the tree pane and select **Hash** from the context menu that appears. Click **OK** to start the hashing process which takes about 2-3 minutes. Record the hash value and compare it with the hash value generated during the Acquire process. You can easily copy and paste the results from that screen. If done properly, it will match the Hash value generated during the Acquire process.

_____

Once you are finished with the lab, everything must be reset back to its original configuration. First, switch the Forensic Computers Drive Power Switch to the off position and disconnect the hard drive power cord and IDE Bridge. Reinstall the hard drive chassis back into the original Dell computer and reconnect the IDE and power cables to the hard drive. Don't forget to attach the screw that holds the chassis in place. Lastly, place the cover back on the Dell computer in reverse order that it was removed.