MGS 410/610 Homework #3

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 Forensics workstation, 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 is best to notify law enforcement immediately.

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

The Workstation you will be using is an Alien Ware computer and is labeled FORENSICS on the front. It is inside the room on the left when you walk into Jacobs 323.

***Note:* The forensics machine is not the fastest machine around, be patient with it.**

Identifying and documenting the hard drive

Record the make, model, capacity and other relevant information about the hard drive connected to the write blocker and forensics workstation.

____

____

____

Using the hardware write blockers

Hardware write blockers are used to prevent any data from being written to the suspect's hard drive during the imaging (copying) process. The necessary write blocker cables, power supply and bridge are already set out on the forensics bench for you and connected to the hard drive and forensics workstation.

Login to the Forensics machine (on the right) with the credentials below:

- Username **Forensics** and password **mgtMSS100**.

If necessary, switch the write blocker (labeled Tableau Firewire 800 + USB 2.0 SCSI Bridge) to the "**A On**" position. You will hear the hard drive begin to make a whirring noise and some clicks as it powers up.

Although the drive is connected, The PC won't be able to recognize it as another device (drive) attached to the computer. The Drive may not be formatted as a hard drive & Windows XP does not have plug and play functionality built in, so the drive is not recognized in windows without the proper formatting and a driver from a CD-ROM.

Based on, your knowledge about write blockers or some Googling: if a generic text file is to be copied from the desktop to the drive, would the file be copied while it is connected to the write blocker? What do you think will happen and why? Also, why would writing files to a drive you are forensically analyzing be a bad thing?

____

____

Imaging and verifying (hashing) the hard drive image

Instructions:

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**. If an error message appears, click the **Continue** Button. This message will appear twice or three times so click **Continue** again. Select the drive (You will need to look for the name of the drive Ex: Seagate) of the hard drive and click **Next**.

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

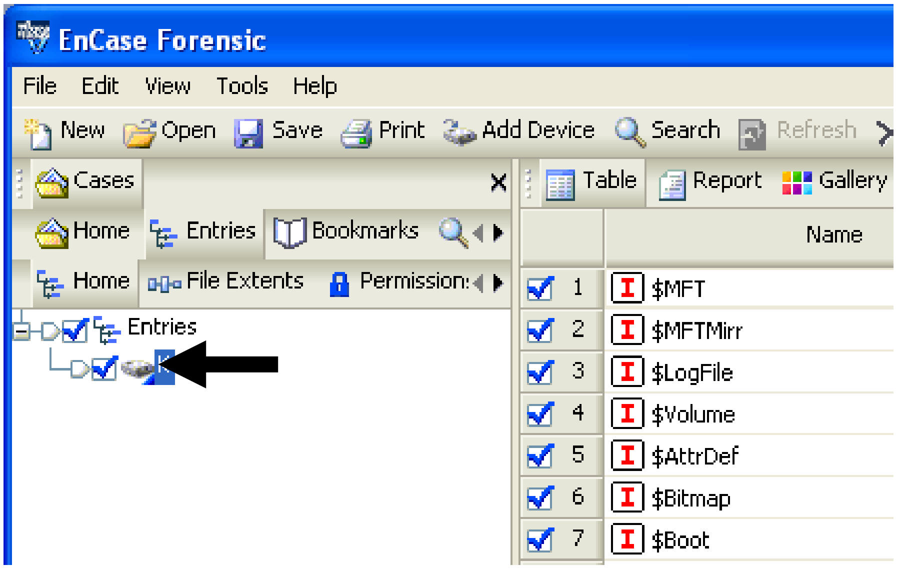
____

____

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).


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks
Home File Extents Permission:
Entries
Table Report Gallery

	Name
1	$MFT
2	$MFTMirr
3	$LogFile
4	$Volume
5	$AttrDef
6	$Bitmap
7	$Boot

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 20 minutes. While you're waiting for the drive partition to image, you can research and answer the questions on the following page.

Note: if the drive is taking longer to acquire or hash than expected. Double click on the flashing light that says acquire, cancel the process and start it again.

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 a SCSI hard drive. Identify two other hard drive technologies commonly used today. Hint: Check the write blockers in the storage 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) On a normal basis, the forensic workstation doesn't have Internet connectivity. (However, you might notice that it does at the current moment). Why might the lab administrator cease internet connectivity for this machine?

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 or provide a screenshot of the results.

____

____

____

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 5 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 or paste a screenshot like in the part above. If done properly, it will match the Hash value generated during the Acquire process.

____

____

____

Wrap Up

Once you are finished with the lab, everything must be reset back to its original configuration. First, switch the write blocker (labeled Tableau Firewire 800 + USB 2.0 SCSI Bridge) to the "**B On**" position. You should hear the hard drive power down when you do this.

Next, please **delete any files** created by the imaging process (Check the desktop and delete the extra files that have appeared, they may say something like 2.1 or etc…) and **Log out of the forensics workstation, do not shut it off**.

If you have screenshotted anything and saved it on the workstation, please delete it.