



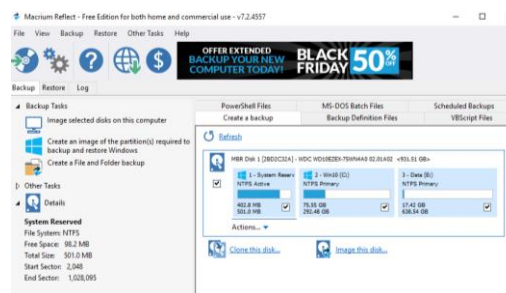
LAB 12 : Business Continuity

1. Creating a Disk Image Backup

One of the trends in backups today is to use disk image programs. A disk image file is created by performing a complete sector-by-sector copy of the hard drive instead of backing up using the drive's file system. It creates a replicated image of the entire drive into a single file, including the operating system and all user files. In this project, will use FTK Imager to create Disk Image backup



Instructions:

1. Use your Web browser to go to <https://www.macrium.com/reflecmcsctfree>
2. Click Home Use and follow the instruction for downloading and installing the software
3. Launch Macrium Reflect



4. In the left pane, click Backup.
5. Click 'Image selected disks on this computer'
6. Choose the disks that you want to backup
7. Choose Desktop as your destination
8. Select 'None' as a template for your backup plan.

9. You can schedule your backup. For this lab activity, no need to schedule the backup
10. You can define your retention rules. For this lab activity, remove all retention rules.
11. Click Next
12. Finish
13. Click OK
14. Check your disk image backup in Desktop
15. Leave Macrium Reflect open for the next project.

- 1.1 Differentiate Full, Differential and Incremental retention rules. 
- 1.2 Differentiate between disk cloning and disk imaging. What is the advantages of disk imaging? 

2. Restoring the Disk Image Backup

It is important to test the steps necessary to restore a disk image in the event that a hard drive stops functioning. In this project, you go through the steps of restoring the Macrium Reflect image backup

Instructions:

1. In the left pane, click Restore.
2. Browse for an image or backup file to restore
3. Choose the image or backup file
4. Click Restore Image
5. Select the destination to restore the disk image
6. Click next
7. Finish

3. Entering and Viewing Metadata


Although most file metadata is not accessible to users, users can enter and change some types of metadata. In this project, you view and enter metadata in a Microsoft Word document.


Instructions:

1. Use Microsoft Word to create a document containing your name. Save the document as Metadata1.docx.
2. Click Properties at the top of the page, and then select Advanced Properties.
3. Click tab Summary

Enter the following information:

- Subject—Metadata
 - Author—The name of your instructor or supervisor
 - Category—Computer Forensics
 - Keyword—Metadata
 - Comments—Viewing metadata in Microsoft Word
4. Click Properties at the top of the page, and then select Advanced Properties.
 5. Click the Statistics tab and view the information it contains.
 6. Click the Custom tab. Notice that there are several predefined fields that can contain metadata.
 7. In the Name box, enter Reader.
 8. Be sure the Type is set to Text.
 9. Enter your name in the Value field, and then press Enter.
 10. Save your document when you are finished.
 11. Close the Document Properties Information panel and return to Metadata1.docx.
 12. Erase your name from Metadata1.docx so you have a blank document.
 13. However, this file still has the metadata. Enter today's date and save this as Metadata2.docx.
 14. Close Metadata2.docx.
 15. Reopen Metadata2.docx.
 16. Click File tab and then Info. Click Properties at the top of the page, and then select Advanced Properties to display the Document Information Panel.

3.1. How could a computer forensics specialist use this metadata when examining this file? 

3.2 What properties carried over to Metadata2.docx from Metadata1.docx, even though the contents of the file were erased? Why did this happen? Could a computer forensics specialist use this technique to examine metadata, even if the contents of the document were erased? 

4. Viewing and Changing the backup Archive Bit

One of the keys to backing up files is to know which files need to be backed up. Backup software can internally designate which files have already been backed up by setting an archive bit in the properties of the file. A file with the archive bit cleared (set to 0) indicates that the file has been backed up. However, when the contents of that file are changed, the archive bit is set (to 1), meaning that this modified file now needs to be backed up. In this project, you view and change the backup archive bit.

Instructions:

1. Start Microsoft Word and create a document that contains your name and today's date.
2. Save this document as Bittest.docx, and then close Microsoft Word.
3. Click Start, type cmd, and then press Enter. The Command Prompt window opens.
4. Navigate to the folder that contains Bittest.docx.
5. Type attrib/? and then press Enter to display the options for this command.
6. Type attrib Bittest.docx and then press Enter. The attributes for this file are displayed.
The A indicates that the bit is set and the file should be backed up.
7. You can clear the archive bit like the backup software does after it copies the file. Type
attrib -a Bittest.docx and then press Enter.
8. Now look at the setting of the archive bit. Type attrib Bittest.docx and then press Enter.
Has it been cleared?
9. Close the Command Prompt window.