Lab 6 – Examining a FAT32 Image

FAT32 supports disk drives up to 2 terabytes and filenames up to 255 characters. It's supported by all versions of Windows (except some 95), Linux and Mac OS X. In this lab we are looking to learn how to examine a FAT32 dd image in FTK Imager and identify a FAT32 file signature.

Activity

1. Copy the file C3Proj2.001 from the Data files to your Work\Labs folder
2. Open FTK Imager and click Yes in the UAC message box
3. Click File, Add Evidence Item. In the source dialog box click the Image file option button and then click Next
4. In the Evidence Source selection box, click Browse, navigate to and click your Work\Labs folder, click Open. Click Finish to load the file.
5. The lower-right pane identifies the file system as MSDOS5.0 FAT32. Expand C3Proj2.001 to select it. The properties pane shows the file in its raw state (dd) and the original disk geometry as 512 bytes per sector with a total of 249,341 sectors.
6. Click the HEX toolbar button to display the hex values for each file. Click the Bank Location.doc file, view its hex information and review its properties. The file signature and file size are the same as in FAT16 however the start cluster and start sector are different than in FAT16.
7. Click the interior safe.jpg file in the File List pane and notice the JFIF file signature for a JPEG file. Click the eyeglass toolbar button to see the file in the image viewer.
8. Click to expand the USBDEVICE [FAT32] folder, if necessary, and examine the FAT32 file structure and all the files in it. Make the screen capture (Ctrl+Print Screen) and paste into WordPad or similar. Save the file in the Documents folder with the filename Structures and exit WordPad. Close FTK.

Lab 7 – Examining an NTFS File

NTFS is the default file system in most Windows Oss because it includes file attributes such as compression and encryption that are not in FAT16/32. NTFS is considered more reliable because of file structures that support redundancy such as a duplicate Master File Table (MFT) and journaling. NTFS also supports file encryption based on user account information so that multiple users on the same computer can't open each other's encrypted files.

Activity

1. Copy the file C3Proj3.001 from the Data files to your Work\Labs folder
2. Open FTK Imager and click Yes in the UAC message box
3. Click File, Add Evidence Item. In the source dialog box click the Image file option button and then click Next
4. In the Evidence Source selection box, click Browse, navigate to and click your Work\Labs folder, click Open. Click Finish to load the file.
5. The lower-left pane identifies the file system as NTFS. Expand C3Proj3.001 and USBDEVICE [NTFS] in the evidence tree pane and click C3Proj3.001 to select it. The properties pane shows the file in its raw state (dd) and the original disk geometry as 512 bytes per sector with a total of 251,904 sectors.
6. Click the [root] folder. The file list pane shows the files in the CP3Proj3.001 image and their timestamps. Notice that NTFS has additional hidden folders for bad cluster identification ($BadClus) and two copies of the MFT ($MFT and $MFTMrr).
7. Click each deleted file (red x) to view it. Notice the NTFS uses a Date Accessed field in addition to the Date Created and Date Modified fields.
8. Click the HEX toolbar button to display the hex values for each file. Click the Bank Location.doc file, view its hex information and review its properties. The file signature and file size are the same as in FAT16/32 however the start locations are different.
9. Click the interior safe.jpg file in the File List pane and notice the JFIF file signature for a JPEG file is the same as the FAT16/32 file signatures for JPEG files. In addition NTFS displays Exif file data with information on a digital camera's model and manufacturer as well as its shutter speed, lens aperture and ISO speed. This info can be useful for an investigation.
10. Notice the complex file structure of the [root] folder, compared with other file systems. Expand all the subfolders under[root] to see, for example, the $Secure attribute indexes that support NTFS file permissions and the [orphan] folder used to repair files broken pointers or corrupted indexes.
11. Make the screen capture (Ctrl+Print Screen) and paste into WordPad or similar. Save the file in the Documents folder in the Structures file and exit WordPad. Close FTK.

Lab 8 – Examining a HFS+ Image

HFS+ is the file system for MAC OS X 10.4 or later, maintains a journal similar to NTFS to keep track of file changes attempted but not completed because of file errors or hard disk crashes. It allows the system to recover from sudden disk crashes or power losses during a write operation. HFS+ is less susceptible to corruption caused by broken or missing pointers because blocks of data on a storage device.

Activity

1. Copy the file C3Proj3.001 from the Data files to your Work\Labs folder
2. Open FTK Imager and click Yes in the UAC message box
3. Click File, Add Evidence Item. In the source dialog box click the Image file option button and then click Next
4. In the Evidence Source selection box, click Browse, navigate to and click your Work\Labs folder, select file and click Open. Click Finish to load the file.
5. Expand C£Proj4.001 and USBDEVICE [HFS+] in the evidence tree pane and click CP3Proj4.001 to select it. The properties pane shows the file in its raw state (dd) and the original disk geometry as 512 bytes per sector with a total of 249,228 sectors.
6. Expand the USBDEVICE folder in the Evidence tree pane. The file list pane shows that files in the C3Proj4.001 image and their timestamps. Notice that there is no [root] folder. Examine the hidden folders (.journal and .journal_info_block) used for journaling file transaction. The properties pane also shows the UNIX permissions for the USBDevice folder: read, write, delete and modify.
7. Expand the .Trashes folder and click the 501 folder. You should see the same deleted files you have seen in previous labs, but HFS+ doesn't add red x's to indicate they were deleted.
8. Click each file with an extension to view its properties and security attributes. The properties pane lists a Date Accessed field in addition to the Date Created and Date Modified fields.
9. Click the HEX toolbar button to display the hex values for each file. Click the Bank Location.doc file, view its hex information and review its properties. The file signature and file size are the same as in FAT16/32 and NTFS however the start locations are different
10. Click the interior safe.jpg file in the File List pane and notice the JFIF file signature is the same as the FAT16 and FAT32. HFS+ also displays EXif file data as NTFS does.
11. Examine the USBDevice folder. Make the screen capture (Ctrl+Print Screen) and paste into WordPad or similar. Save the file in the Documents folder in the file Structures and exit WordPad. Close FTK.