File System Attributes Exercise

BitCuratorEdu

Last Updated: January 18, 2022

About This Exercise

Author

Cal Lee

Description

This hands-on exercise is meant to introduce students file systems and interpreting file system attributes. These slides are excerpted from Cal Lee's SAA "Advanced Digital Forensic" class. The sample data referenced in these slides is available here: https://github.com/BitCurator/bcc-dfa-sample-data/

Learning object type

Lesson plan/materials

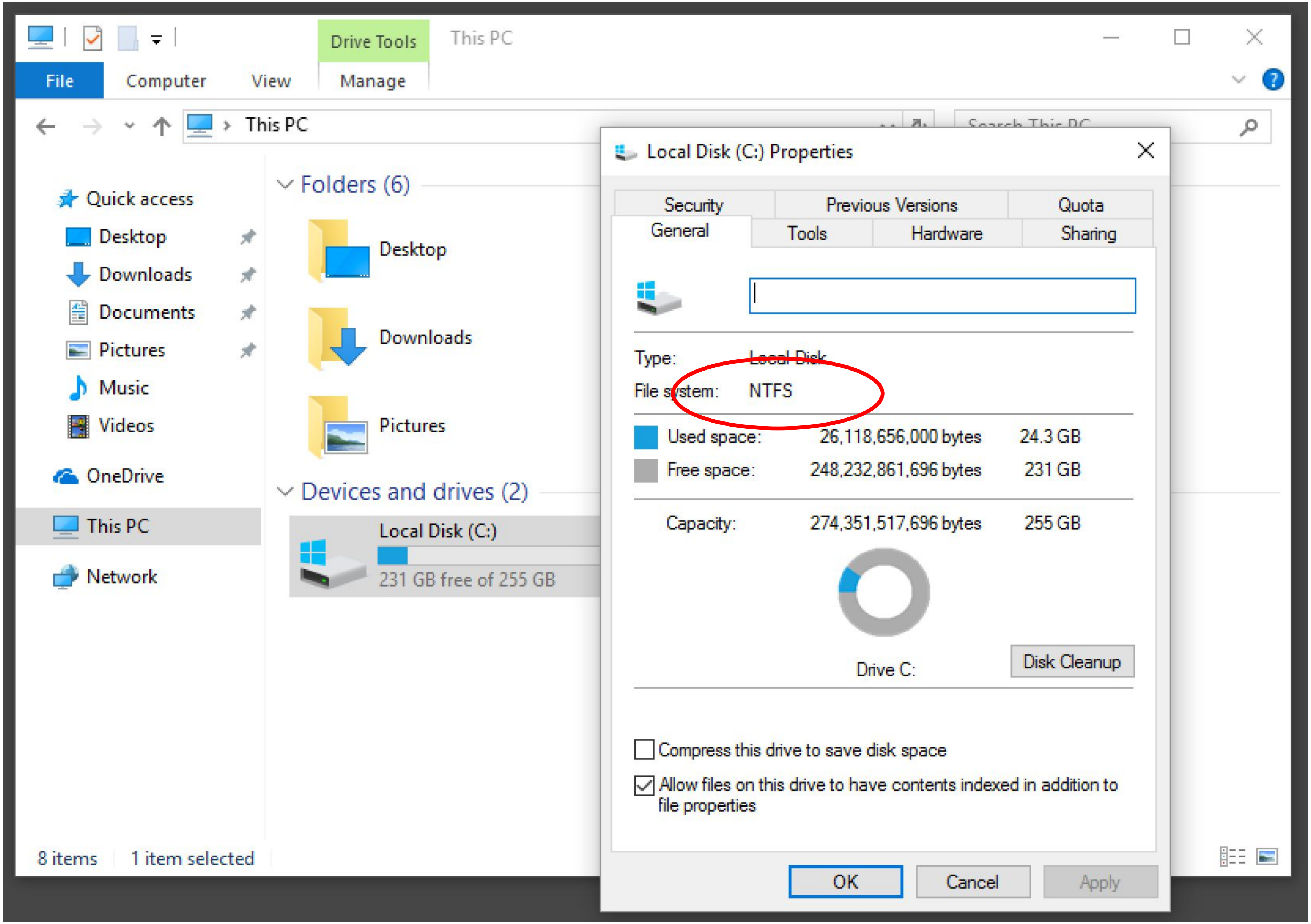
Learning objectives

This learning object might be used in a lesson to satisfy the following learning objectives:

- Practice using tools in the BitCurator Environment.

File System

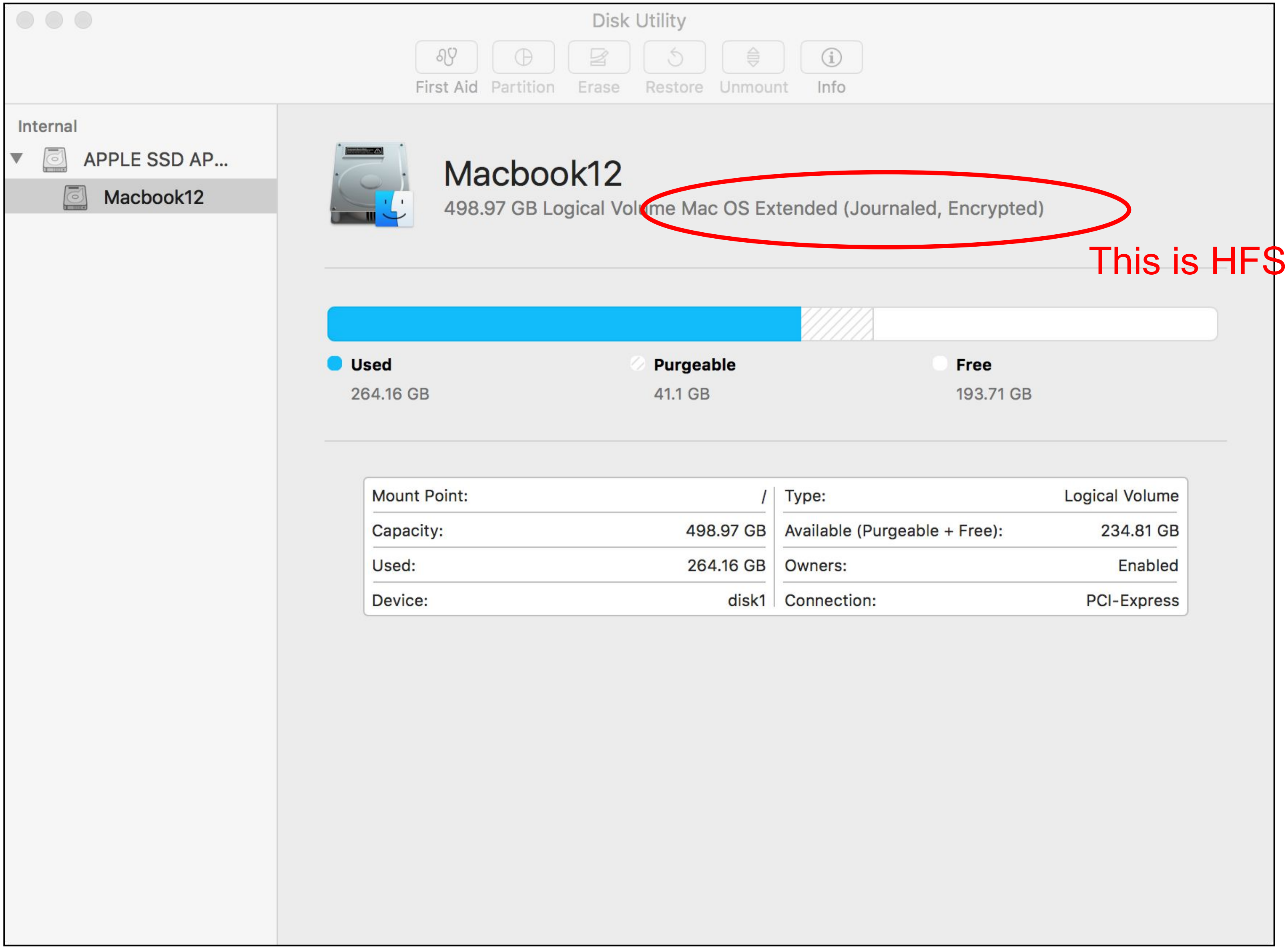
- Access controls
- File names & identifiers
- File size (length)
- Where to find files in storage (sectors and clusters)
- MAC times
  - Modified – when the content was last changed
  - Accessed – time file was last accessed (by person or software)
  - Changed – last time metadata changed
  - Created – (implemented inconsistently, if at all, across different file systems)



Type:	Local Disk	
File system:	NTFS	
Used space:	26,118,656,000 bytes	24.3 GB
Free space:	248,232,861,696 bytes	231 GB
Capacity:	274,351,517,696 bytes	255 GB

□ Compress this drive to save disk space

☑ Allow files on this drive to have contents indexed in addition to file properties



Macbook12

498.97 GB Logical Volume Mac OS Extended (Journaled, Encrypted)

This is HFS+

● Used
264.16 GB

▨ Purgeable
41.1 GB

○ Free
193.71 GB

Mount Point:	/	Type:	Logical Volume
Capacity:	498.97 GB	Available (Purgeable + Free):	234.81 GB
Used:	264.16 GB	Owners:	Enabled
Device:	disk1	Connection:	PCI-Express

File System Examples

Name	Operating System(s) Using it as Native File System [often other OSs can also recognize it]
FAT12, FAT16	MS-DOS
FAT32 (VFAT)	Windows 95, 98
exFAT	Windows XP SP2 and later (primary use: USB drives, SD cards)
NTFS	Windows NT, 2000, XP, Server 2003, Server 2008, Vista
MFS	Macintosh System 1-3
HFS (Hierarchical File System)	Macintosh System 4-8
HFS+	Macintosh System 8.1 – 9, OS X 10.0 – 10.11
APFS	macOS 10.12
ext, ext2, ext3, ext4 (Extended File System)	Linux
XFS	Linux, typically Enterprise variants (RHEL)
HPFS (High Performance File System)	OS/2
ISOFS (ISO 9660)	Any OS that reads data from a CD
JFS1 (Journaled File System)	AIX (IBM)
ReiserFS	Several Linux distributions
UFS (Unix File System) aka FFS (Fast File System)	Various flavors of Unix

File System Examples

Name	Operating System(s) Using it as Native File System [often other OSs can also recognize it]
FAT12, FAT16	MS-DOS
FAT32 (VFAT)	Windows 95, 98
exFAT	W
NTFS	W
MFS	M
HFS (Hierarchical File System)	M
HFS+	M
APFS	m
ext, ext2, ext3, ext4 (Extended File System)	Li
XFS	Li
HPFS (High Performance File System)	OS/2
ISOFS (ISO 9660)	Any OS that reads data from a CD
JFS1 (Journaled File System)	AIX (IBM)
ReiserFS	Several Linux distributions
UFS (Unix File System) aka FFS (Fast File System)	Various flavors of Unix

Filesystems you’re most likely to encounter

NTFS vs. FAT Filesystem Attributes

- Download these two disk images (or use the copies from the flash drives):

  https://github.com/BitCurator/bcc-dfa-sample-data/blob/main/terry-work-usb-2009-12-11.E01

  https://github.com/BitCurator/bcc-dfa-sample-data/blob/main/ntfs1-gen1.E01

- Load each disk image into a separate instance of FTK Imager (run them side by side to compare what you see) – if you don't have a Windows computer, look on with a partner
- Look at the properties of some files*
- What differences do you notice?

*Properties are shown in the bottom left corner. If you don't see them, go to the View menu at the top and select "Properties." You may need to drag the top of the properties window up to see all of the values.

BitCuratorEdu

Advancing the adoption of digital forensics tools and methods in libraries and archives through professional education efforts

This resource was released by the BitCuratorEdu project and is licensed under a Creative Commons Attribution 4.0 International License.

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

The BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.