Lab 3: The NTFS File System

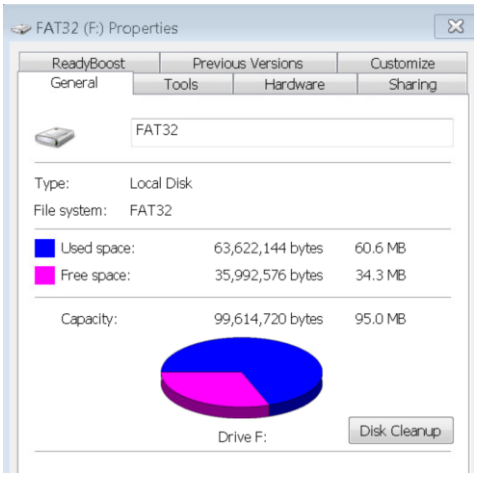
Objective:

Gain fundamentals within digital forensics. Students will demonstrate understandings of forensic methodology, identifying types of evidence on current Windows OS and be familiar with structure and composition of modern Windows file systems.

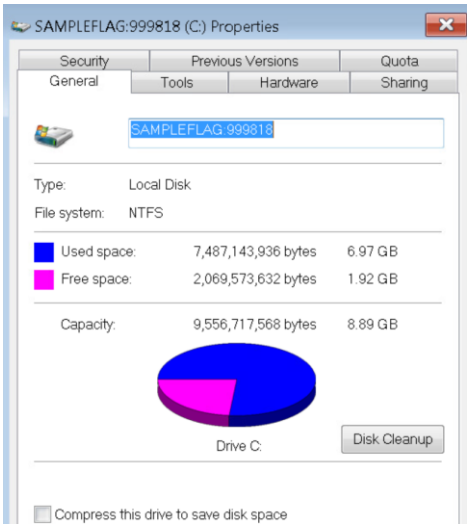
Terms:

- NTFS
    - New technology file system introduced in Windows NT. It is a journaling file system meant to keep logs of changes on a written disk. If a computer shuts down improperly, it has a chance to recover due to this.
- EFS
    - Feature of NTFS allowing you to encrypt files and folders. Became available in 2000 and is still available today on Windows 10.
- ADS
    - Alternate Data Stream
        - Feature of NTFS that allows compatibility with older versions of Mac OS. It is utilized when individuals attempt to hide data on their system with an NTFS volume
- Timestomp
    - Command that changes file modifications, access, and created times. Can only change MAC times on an NTFS volume.
- $MFT
    - Master file table that is essentially the table of contents for an NTFS volume.

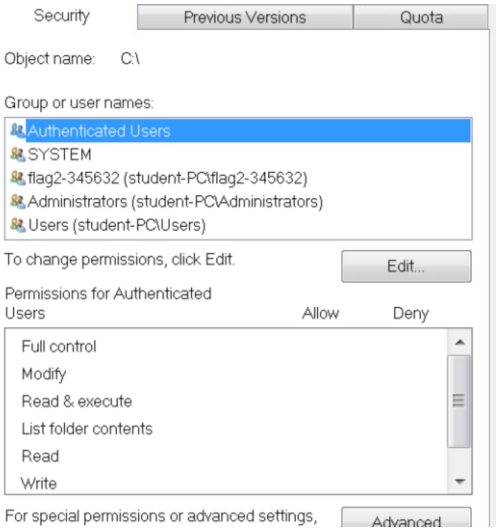
Step 1: Examining NTFS Features



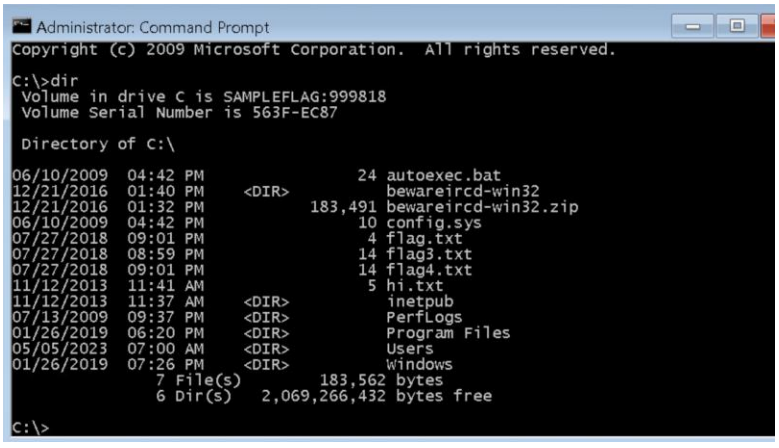
- Examining a FAT32 drive. No security tab.



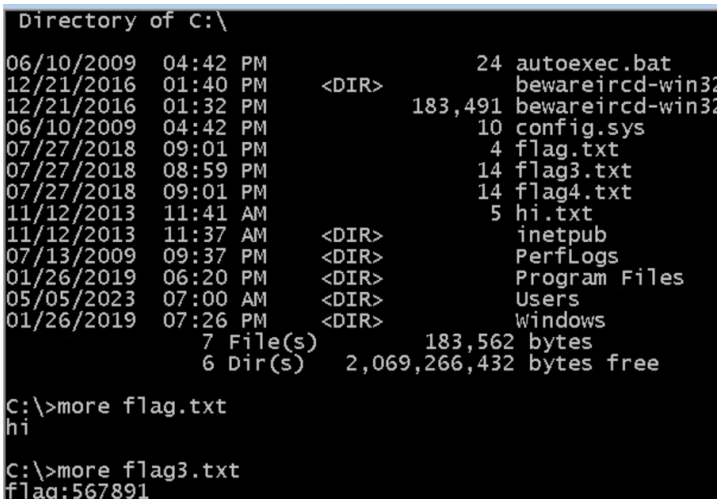
- Viewing NTFS local drive with a security tab and flag in the name

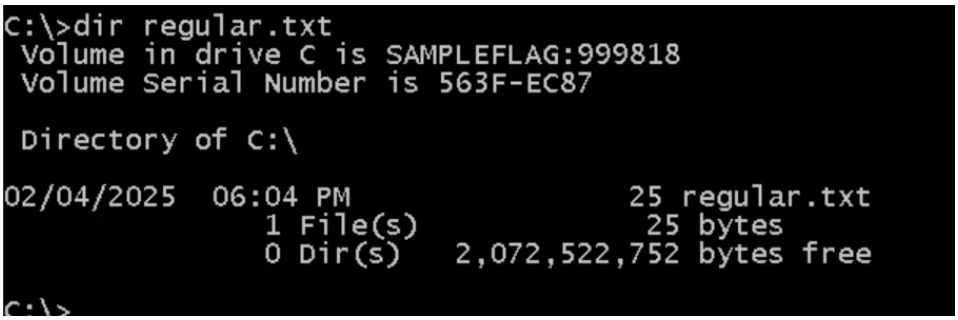


- Examining security tab and finding flag 2. This area displays access controls
- Quota
    - This tab is where disk usage can be restricted.



- Asked to execute “dir”, a command that appears to list a set of files and directories.

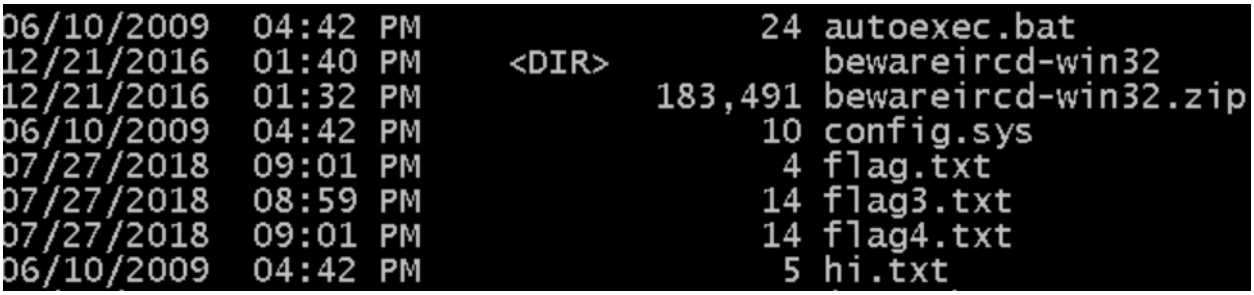




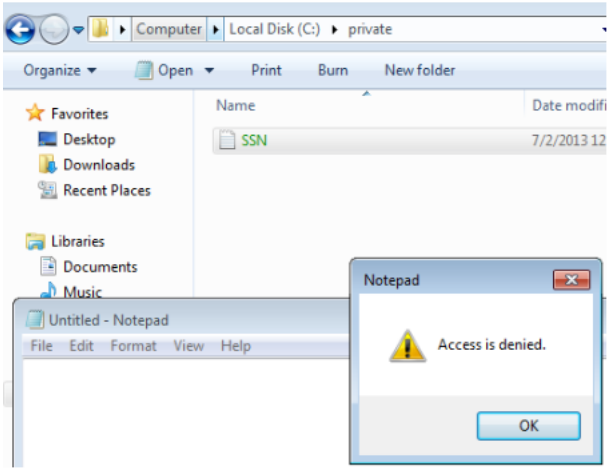
- We’ve created a regular and hidden txt file. This displays information on the regular file before we hide the hidden.txt within the regular using an alternate data stream.

- Use “dir /r” to display ADS files on root.
- Executed timestomp command

C:\>timestomp hi.txt –f config.sys

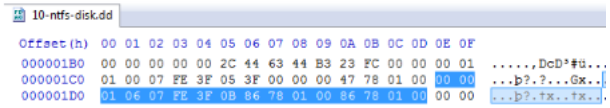


```
05/05/2023  07:00 AM    <DIR>          Users
01/26/2019  07:26 PM    <DIR>          Windows
               7 File(s)        183,562 bytes
               7 Dir(s)   2,072,514,560 bytes free

C:\>cd private

C:\private>echo 123-45-6789 > SSN.txt

C:\private>dir
 Volume in drive C is SAMPLEFLAG:999818
 Volume Serial Number is 563F-EC87

 Directory of C:\private

02/04/2025  06:28 PM    <DIR>          .
02/04/2025  06:28 PM    <DIR>          ..
02/04/2025  06:28 PM                14 SSN.txt
               1 File(s)             14 bytes
               2 Dir(s)   2,072,514,560 bytes free

C:\private>type SSN.txt
123-45-6789
```

- Appears we've added users jessejames with password cowboy.
- 

    - We created a file on the previous user and added some restrictions to the new user account.

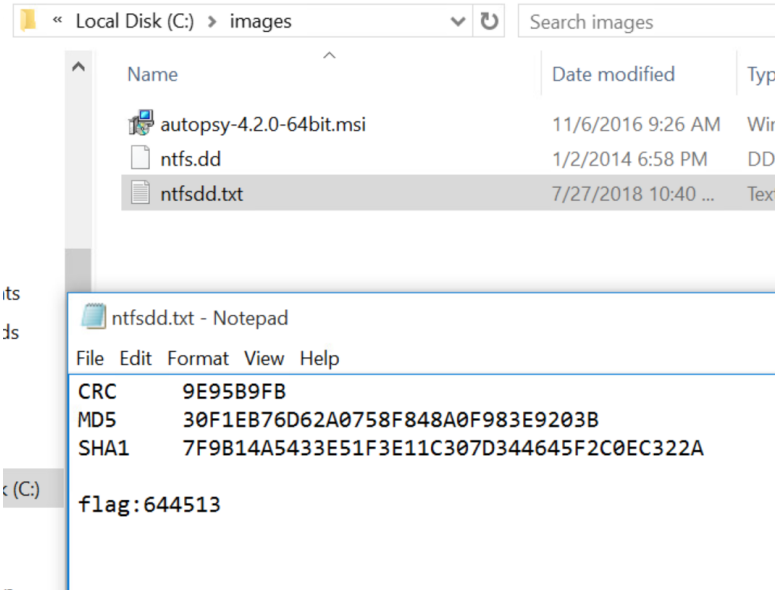
Using a HEX Editor to Explore NTFS Partitions

- Using HxD to examine 00000000 – 00000162
- Found Missing Operating System in Hex
- First partition begins at 1BE to 1CD and is 16 bytes long
- Standard DOS systesm can have up to 4 primary partitions.
- 

    - One of four partitions.
    - The first byte indicates if it is bootable. 00 indicates non-bootable while a value of 80 is bootable.
    - 01, 01, 00, indivate sector and cylinder (CHD address).

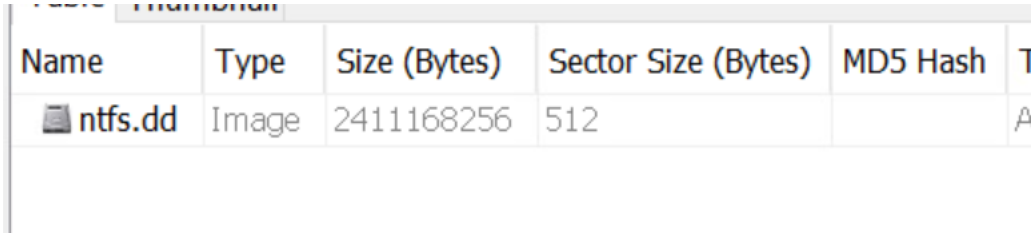
Verifying and Viewing Image Details

- Images are bit by bit copies of a disk.

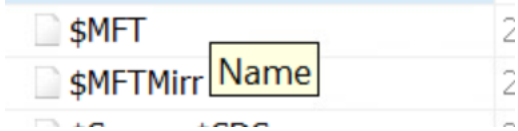


- Viewing ntfsdd.txt info through local disk.
- We then view properties of the .dd file and view the hashes to confirm they match.

Analyzing NTFS Partition with Autopsy



- Created case with Autopsy



-
  - Includes these in the NTFS system.