

Lab 3: The NTFS File System

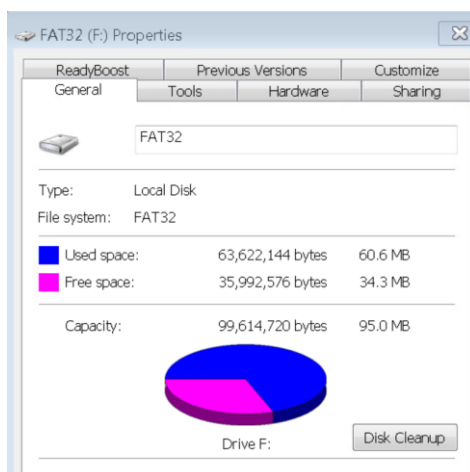
Objective:

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.

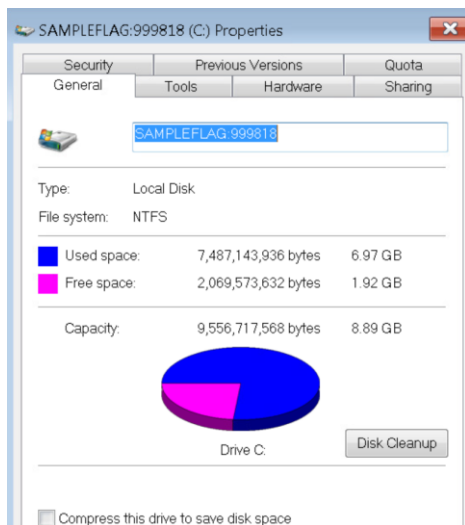
Terms:

- NTFS
 - o 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
 - o Feature of NTFS allowing you to encrypt files and folders. Became available in 2000 and is still available today on Windows 10.
- ADS
 - o 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
- Timestamp
 - o Command that changes file modifications, access, and created times. Can only change MAC times on an NTFS volume.
- \$MFT
 - o Master file table that is essentially the table of contents for an NTFS volume.

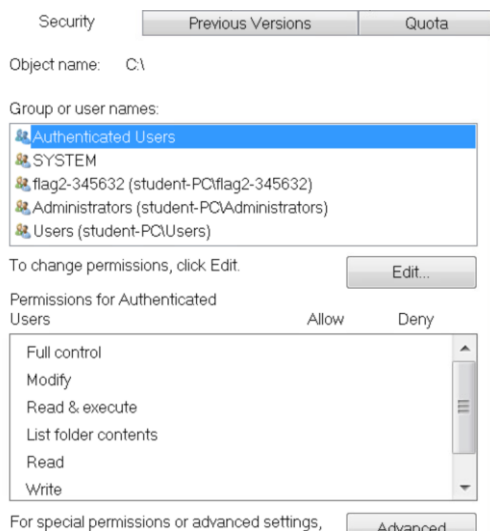
Step 1: Examining NTFS Features



- 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
 - o This tab is where disk usage can be restricted.

```
Administrator: Command Prompt
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

Directory of C:\

06/10/2009  04:42 PM                24 autoexec.bat
12/21/2016  01:40 PM            <DIR>         bewareircd-win32
12/21/2016  01:32 PM       183,491 bewareircd-win32.zip
06/10/2009  04:42 PM                10 config.sys
07/27/2018  09:01 PM                 4 flag.txt
07/27/2018  08:59 PM                14 flag3.txt
07/27/2018  09:01 PM                14 flag4.txt
11/12/2013  11:41 AM                 5 hi.txt
11/12/2013  11:37 AM            <DIR>         inetpub
07/13/2009  09:37 PM            <DIR>         PerfLogs
01/26/2019  06:20 PM            <DIR>         Program Files
05/05/2023  07:00 AM            <DIR>         Users
01/26/2019  07:26 PM            <DIR>         Windows
              7 File(s)        183,562 bytes
              6 Dir(s)      2,069,266,432 bytes free

C:\>
```

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

```

Directory of C:\
06/10/2009  04:42 PM                24 autoexec.bat
12/21/2016  01:40 PM             <DIR>      bewareircd-win32
12/21/2016  01:32 PM      183,491 bewareircd-win32.zip
06/10/2009  04:42 PM                10 config.sys
07/27/2018  09:01 PM                 4 flag.txt
07/27/2018  08:59 PM                14 flag3.txt
07/27/2018  09:01 PM                14 flag4.txt
11/12/2013  11:41 AM                 5 hi.txt
11/12/2013  11:37 AM             <DIR>      inetpub
07/13/2009  09:37 PM             <DIR>      PerfLogs
01/26/2019  06:20 PM             <DIR>      Program Files
05/05/2023  07:00 AM             <DIR>      Users
01/26/2019  07:26 PM             <DIR>      Windows
              7 File(s)          183,562 bytes
              6 Dir(s)    2,069,266,432 bytes free

C:\>more flag.txt
hi

C:\>more flag3.txt
flag:567891

```

```

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

Directory of C:\
02/04/2025  06:04 PM                25 regular.txt
              1 File(s)                25 bytes
              0 Dir(s)    2,072,522,752 bytes free

C:\>

```

- 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.

```

C:\>type hidden.txt > regular.txt:hidden.txt

```

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

```

C:\>timestomp hi.txt -f config.sys

```

```

06/10/2009  04:42 PM                24 autoexec.bat
12/21/2016  01:40 PM             <DIR>      bewareircd-win32
12/21/2016  01:32 PM      183,491 bewareircd-win32.zip
06/10/2009  04:42 PM                10 config.sys
07/27/2018  09:01 PM                 4 flag.txt
07/27/2018  08:59 PM                14 flag3.txt
07/27/2018  09:01 PM                14 flag4.txt
06/10/2009  04:42 PM                 5 hi.txt

```

```

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

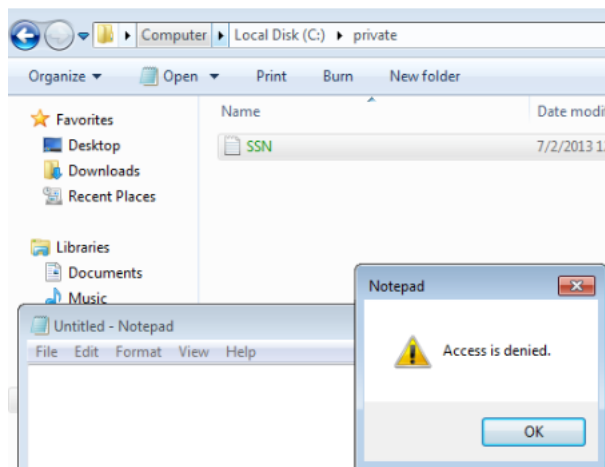
Directory of C:\private

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.



- - o 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 systems can have up to 4 primary partitions.

```

10-ntfs-disk.dd

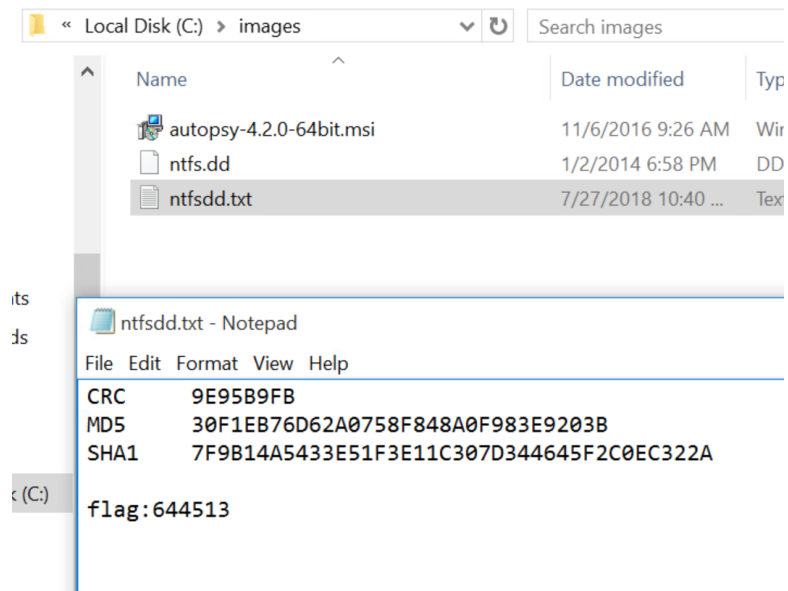
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000001B0 00 00 00 00 00 2C 44 63 44 B3 23 FC 00 00 00 01 .....DcD³#ü...
000001C0 01 00 07 FE 3F 05 3F 00 00 00 47 78 01 00 00 00 ...p?.?...Gx...
000001D0 01 06 07 FE 3F 0B 86 78 01 00 86 78 01 00 00 00 ...p?.?X...TX...

```

- - o One of four partitions.
 - o The first byte indicates if it is bootable. 00 indicates non-bootable while a value of 80 is bootable.
 - o 01, 01, 00, indicate 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

Name	Type	Size (Bytes)	Sector Size (Bytes)	MD5 Hash	1
ntfs.dd	Image	2411168256	512		A

- Created case with Autopsy

\$MFT	2
\$MFTMirr	2

- Includes these in the NTFS system.