

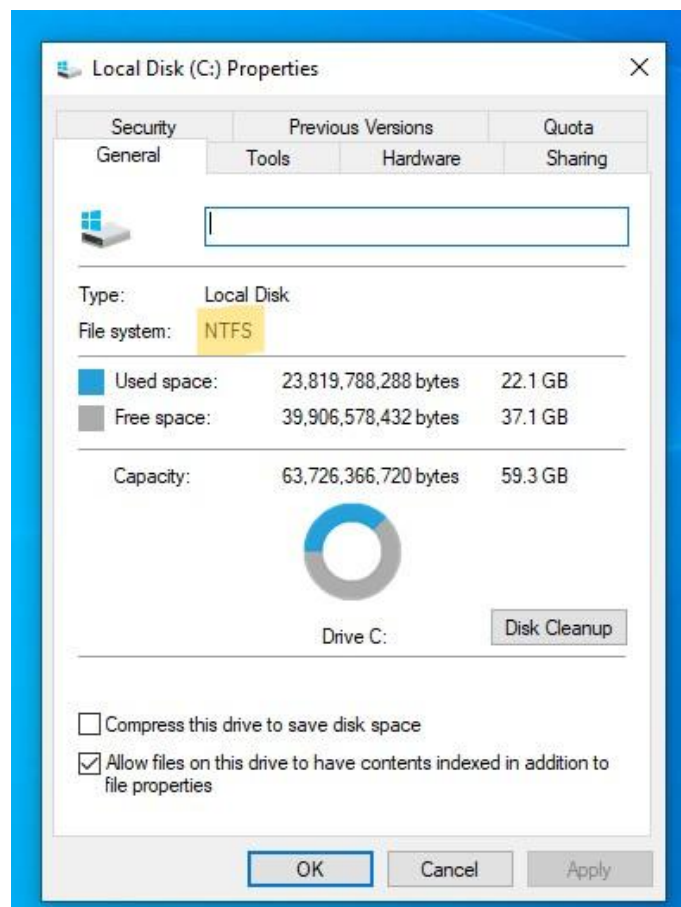
# Hide Files using NTFS Streams

## Introduction :

NTFS (New Technology File System) is the proprietary and default file system for modern Windows operating systems, starting with Windows NT. It was developed to overcome the limitations of its predecessors, such as FAT16 and FAT32, and to meet the growing demands for security, reliability, and performance in both personal and enterprise computing environments.

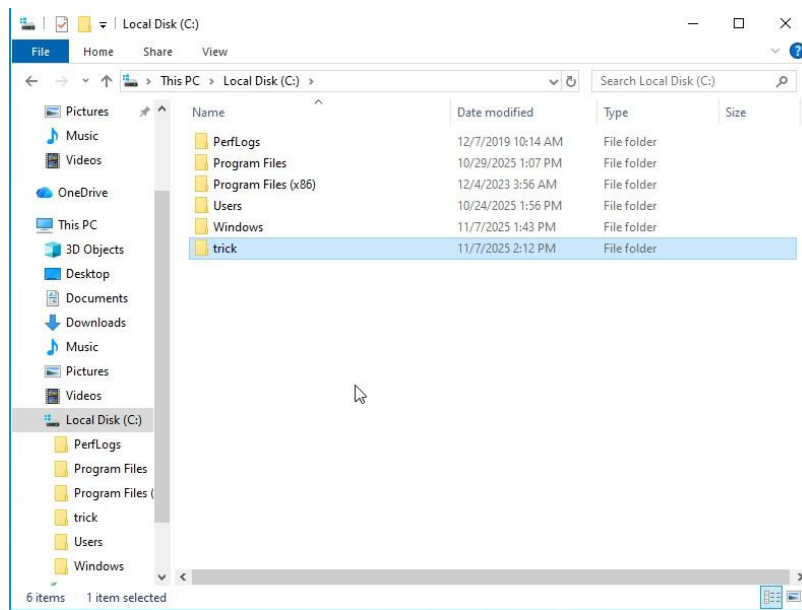
## Step1 :

It has been confirmed that the file system for the (C:) drive is NTFS.



## Step 2 :

A folder named "trick" was successfully created in the root directory of the (C:) drive.

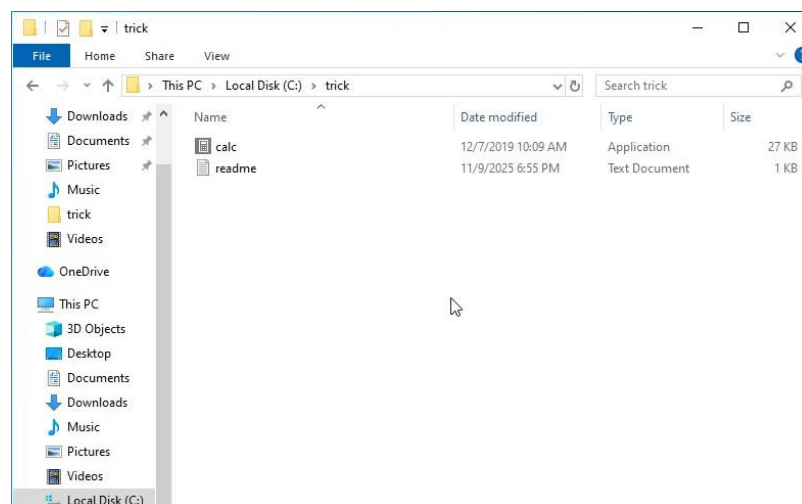


### Step 3 :

Successfully navigated to the "**trick**" folder created in the C: drive.

Inside the folder, two files was created:

- "**calc**" : is a copy of the original calc.exe application from C:\Windows\System32.
- "**readme**" : The file contains the text "Hello World".



### Step 4 :

#### 1. Command: `cd c:\trick`

**Explanation:** This command stands for "Change Directory". It is used to navigate from the current directory (`c:\Windows\system32`) to the `c:\trick` folder.

**Result:** The command prompt changed from `c:\Windows\system32>` to `c:\trick>`, confirming that the user is now working inside the correct directory for the lab.

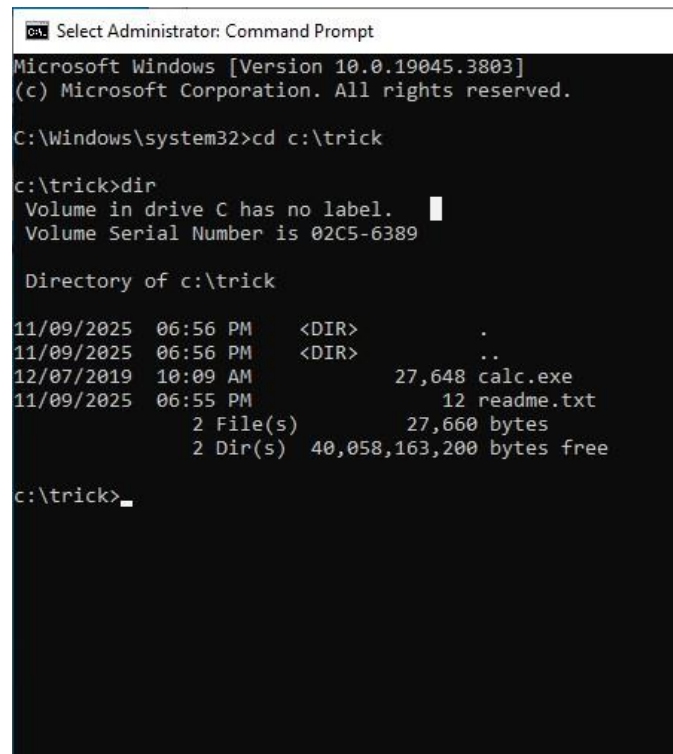
#### 2. Command: `dir`

**Explanation:** This command stands for "Directory". It lists the contents (files and folders) of the current directory.

**Result:** The command displayed the contents of the c:\trick folder, showing two files:

calc.exe: A 27,648-byte (27 KB) application. This is the Windows Calculator copied earlier.

readme.txt: A 12-byte text file. This file contains the text "Hello World".



```
ca. Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c:\trick

c:\trick>dir
Volume in drive C has no label.
Volume Serial Number is 02C5-6389

Directory of c:\trick

11/09/2025  06:56 PM    <DIR>          .
11/09/2025  06:56 PM    <DIR>          ..
12/07/2019  10:09 AM                27,648 calc.exe
11/09/2025  06:55 PM                 12 readme.txt
               2 File(s)              27,660 bytes
               2 Dir(s)  40,058,163,200 bytes free

c:\trick>
```

## Step 5 :

1. Command: `type c:\trick\calc.exe > c:\trick\readme.txt:calc.exe`

**Explanation:**

- type is used to display the content of a file. Here, it reads the binary content of calc.exe.
- The > operator redirects this output.
- The target is readme.txt:calc.exe, which is an Alternate Data Stream (ADS) named calc.exe attached to the file readme.txt.
- **Result:** This command creates a hidden copy of the calc.exe executable inside an ADS of readme.txt. The original readme.txt file remains unchanged in its primary stream.

2. Command: `dir`

- Explanation: Lists the contents of the current directory.
- Result: The output shows no visible change. The directory listing still displays only the two original files (calc.exe and readme.txt) with their original sizes. The hidden ADS (readme.txt:calc.exe) is not visible in a standard directory listing.

```
c:\trick>type c:\trick\calc.exe > c:\trick\readme.txt:calc.exe

c:\trick>dir
Volume in drive C has no label.
Volume Serial Number is 02C5-6389

Directory of c:\trick

11/09/2025  06:56 PM  <DIR>          .
11/09/2025  06:56 PM  <DIR>          ..
12/07/2019  10:09 AM                27,648  calc.exe
11/09/2025  07:07 PM                12      readme.txt
               2 File(s)                27,660 bytes
               2 Dir(s) 39,926,022,144 bytes free

c:\trick>
```

## Step 6 :

### 1. Command: `mklink backdoor.exe readme.txt:calc.exe`

#### Explanation:

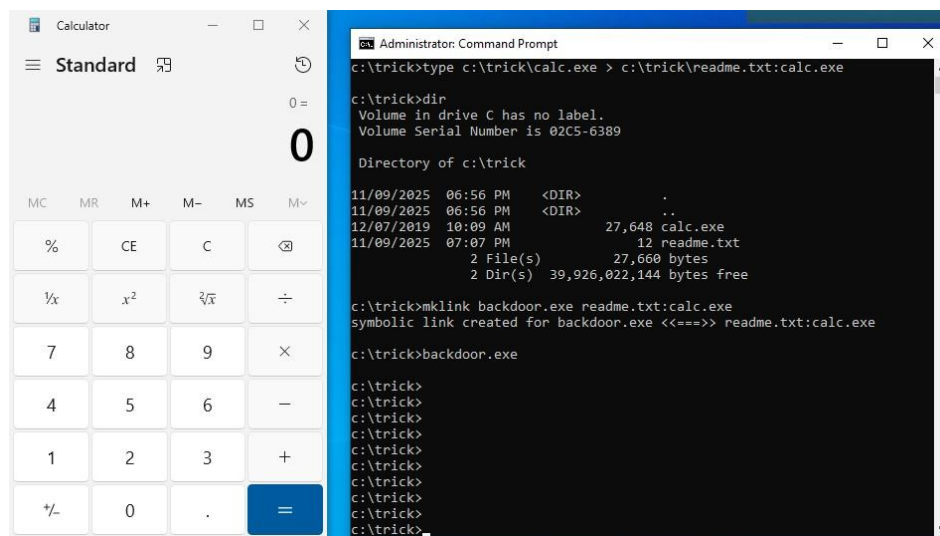
- `mklink` is a command to create a symbolic link.
- `backdoor.exe` is the name of the new link being created.
- `readme.txt:calc.exe` is the target, which is the hidden Alternate Data Stream (ADS) containing the calculator executable.

**Result:** A symbolic link named `backdoor.exe` is created, which points directly to the hidden executable stored in the ADS of `readme.txt`.

### 2. Command: `backdoor.exe`

**Explanation:** This command executes the `backdoor.exe` symbolic link.

**Result:** The Windows Calculator application opens successfully. This proves that the executable hidden in the ADS can be executed normally through the symbolic link.



**Conclusion:**

The lab successfully demonstrates how to execute a program hidden in an NTFS Alternate Data Stream. By creating a symbolic link to the hidden stream (readme.txt:calc.exe), the calculator executable was launched without being visible as a standalone file. This technique shows how malware could be hidden in ADS and executed without detection by ordinary file browsing methods, highlighting a significant security concern of the NTFS file system.