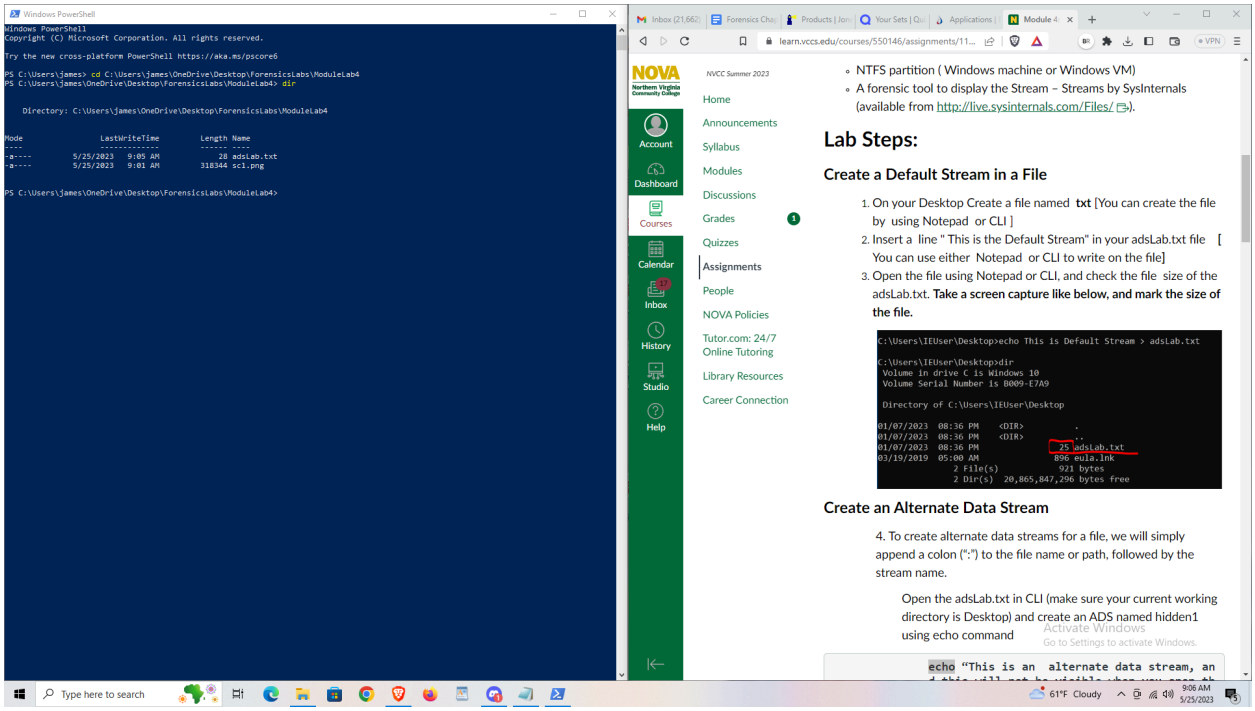
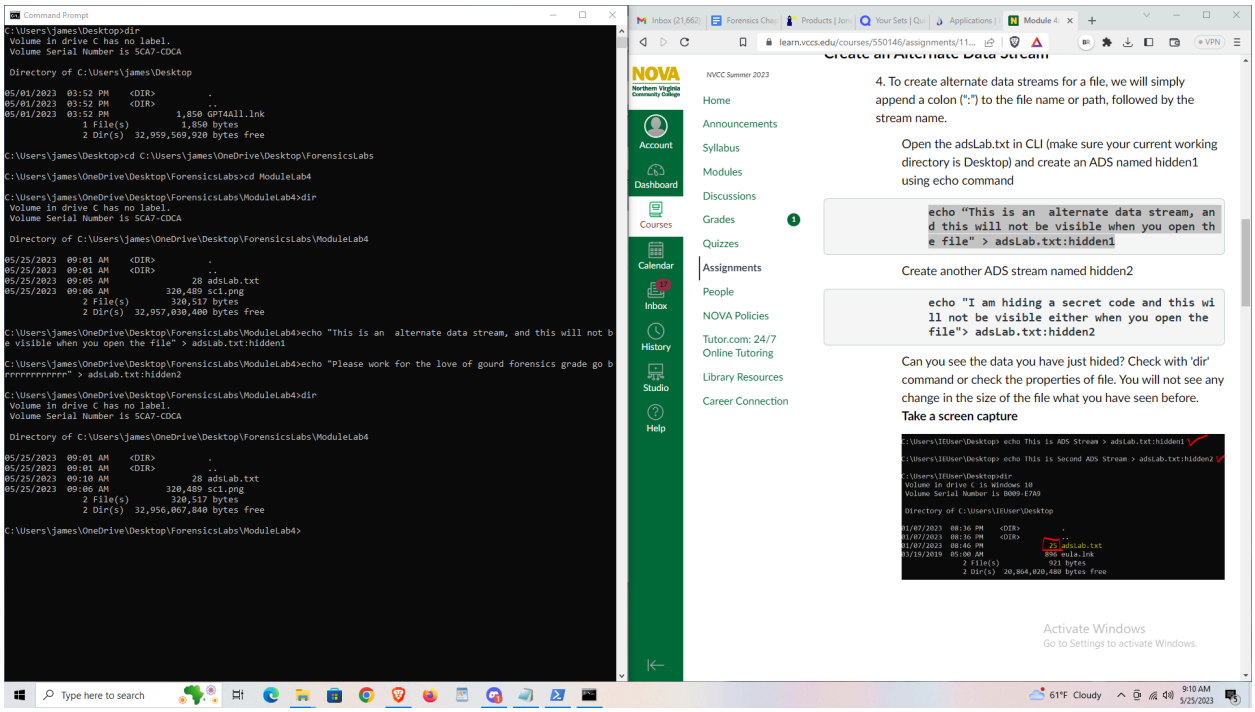
James Tourtellotte
5/27/2023
ITN 276 - Alternate Data Stream in NTFS

Screen Capture 1:

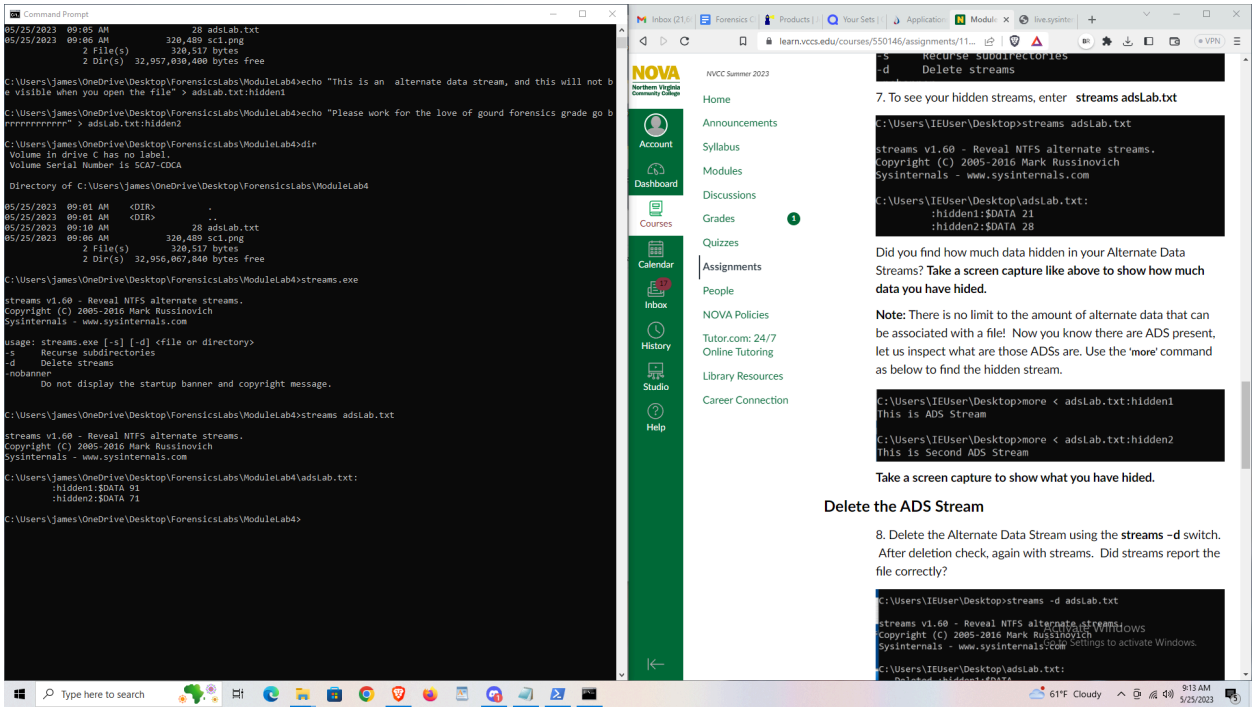
> The size of the file was 28



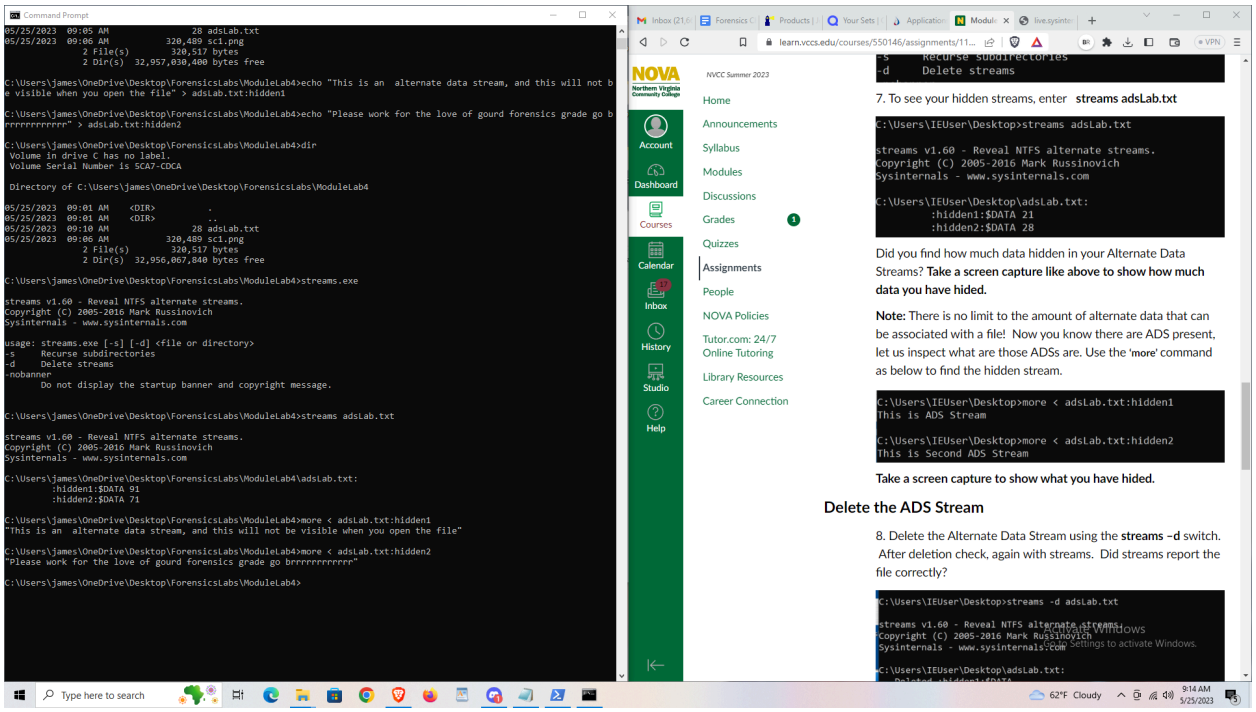
Screen Capture 2:



Screen Capture 3:



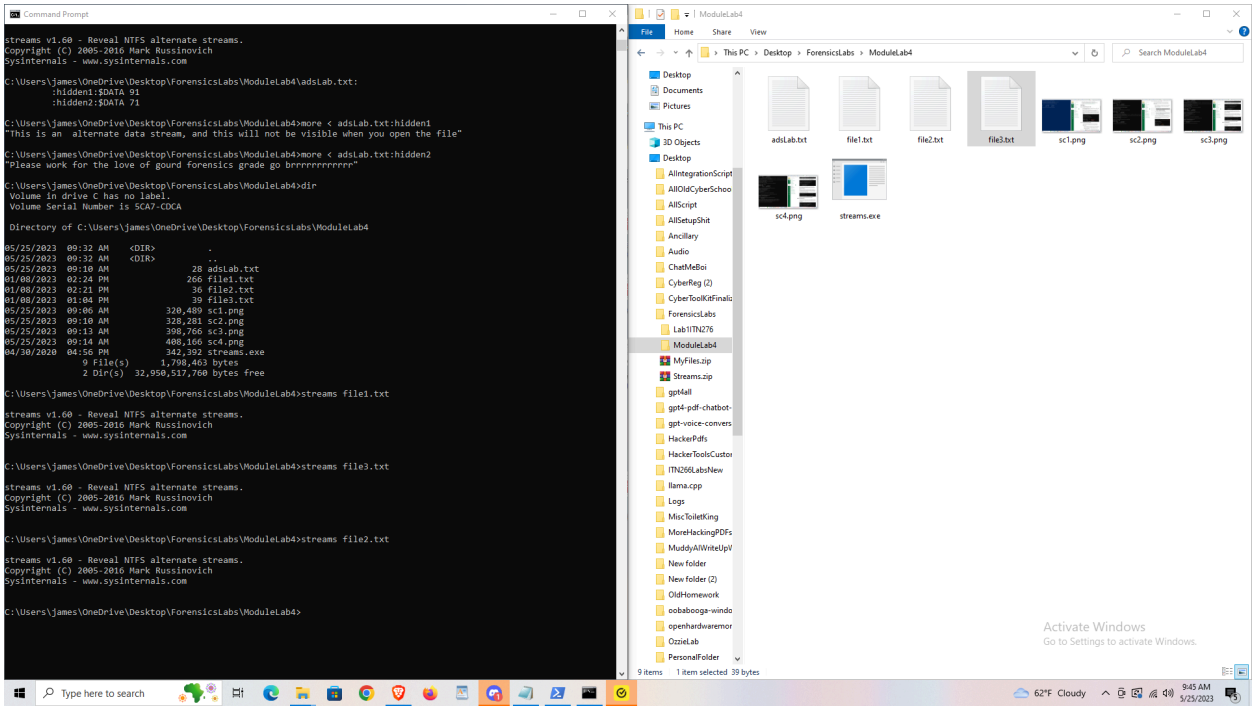
Screen Capture 4:



Screen Capture 5:

3 Files in total, sizes of 39, 36, and 266. File3.txt = 39, File2.txt = 36, File1.txt = 266

I did everything in the lab as stated and no ADS were found.


Command Prompt
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4\adsLab.txt:
:hidden1:$DATA 91
:hidden2:$DATA 71
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>more < adsLab.txt:hidden1
"This is an alternate data stream, and this will not be visible when you open the file"
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>more < adsLab.txt:hidden2
"Please work for the love of gourd forensics grade go brrrrrrrrrrrr"
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>dir
Volume in drive C has no label.
Volume Serial Number is 5CA7-CDCA
Directory of C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4
05/25/2023 09:32 AM <DIR> .
05/25/2023 09:32 AM <DIR> ..
05/25/2023 09:10 AM 28 adsLab.txt
01/08/2023 02:24 PM 266 file1.txt
01/08/2023 02:21 PM 36 file2.txt
01/08/2023 01:04 PM 39 file3.txt
05/25/2023 09:06 AM 320,489 sc1.png
05/25/2023 09:10 AM 328,281 sc2.png
05/25/2023 09:13 AM 398,766 sc3.png
05/25/2023 09:14 AM 408,166 sc4.png
04/30/2020 04:56 PM 342,392 streams.exe
9 File(s) 1,798,463 bytes
2 Dir(s) 32,950,517,760 bytes free
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>streams file1.txt
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>streams file3.txt
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>streams file2.txt
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
C:\Users\james\OneDrive\Desktop\ForensicsLabs\ModuleLab4>
ModuleLab4
File
Home
Share
View
This PC › Desktop › ForensicsLabs › ModuleLab4
Search ModuleLab4
Desktop
Documents
Pictures
This PC
3D Objects
Desktop
AllIntegrationScript
AllOldCyberSchoo
AllScript
AllSetupShit
Ancillary
Audio
ChatMeBoi
CyberReg (2)
CyberToolKitFinalu
ForensicsLabs
Lab1ITN276
ModuleLab4
MyFiles.zip
Streams.zip
gpt4all
gpt-pdf-chatbot-
gpt-voice-convers
HackerPdfs
HackerToolsCustor
ITN266LabsNew
llama.cpp
Logs
MiscToiletKing
MoreHackingPDFs
MuddyAIWriteUpV
New folder
New folder (2)
OldHomework
oobabooga-windo
openhardwaremor
OzzieLab
PersonalFolder
adsLab.txt
file1.txt
file2.txt
file3.txt
sc1.png
sc2.png
sc3.png
sc4.png
streams.exe
9 items
1 item selected 39 bytes
Activate Windows
Go to Settings to activate Windows.
Type here to search
62°F Cloudy
9:45 AM
5/25/2023