

# ITMS 538 Assignment 06a\_s

Alan Palayil

Due Date: 11/28/2022

## Alternate Data Streams

Step 1:

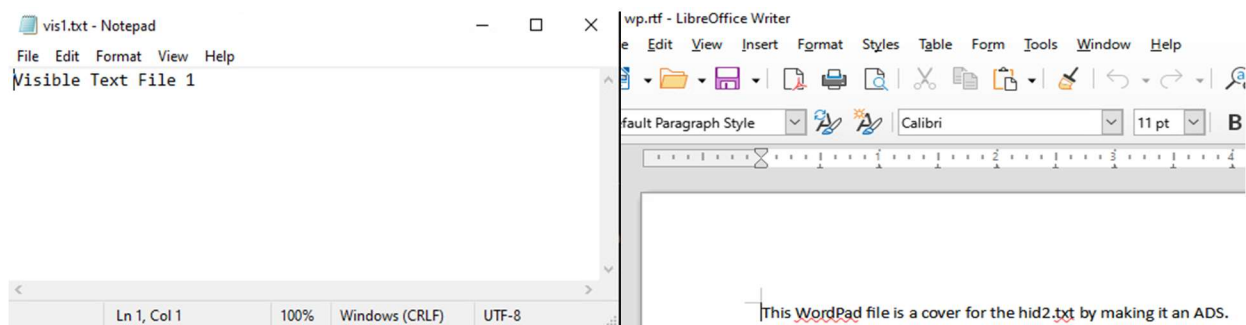
Using the ADS Lab, we first create a folder named ADSLab in C:\Documents. We then run cmd as Administrator and navigate to the ADSLab. We use the following commands to create the labs according to ADS Lab slide 17~20:

```
echo You can't see me > vis1.txt:hid1.txt
```

```
echo Hidden text file 2 > hid2.txt
```

```
type hid2.txt > wp.rtf:hid2.txt
```

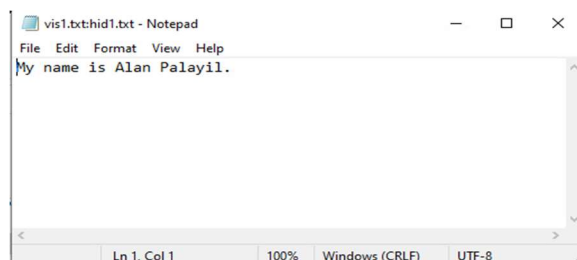
When you click over the visible files:



Once we confirm the texts, we edit the hidden texts according to the Assignment 06a\_s and change hid1.txt to “My name is Alan Palayil.” and hid2.txt to “I was born in Navi Mumbai, India.”

To view the hidden text within the files, we use the following commands:

```
notepad vis1.txt:hid1.txt
```

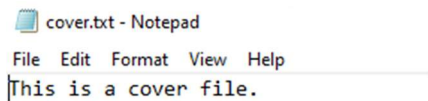


```
more < wp.rtf:hid2.txt
```

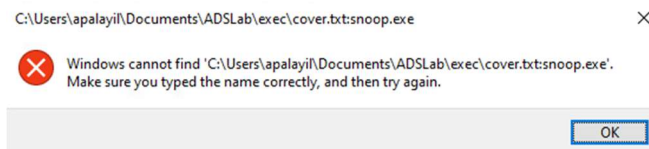
```
C:\Users\apalayil\Documents\ADSLab>more < wp.rtf:hid2.txt  
I was born in Navi Mumbai, India
```

We now create an exec folder and follow the instructions from slide 22~27. We create the files accordingly and try to run them using the following command in the exec folder:

```
start .\cover.txt
```

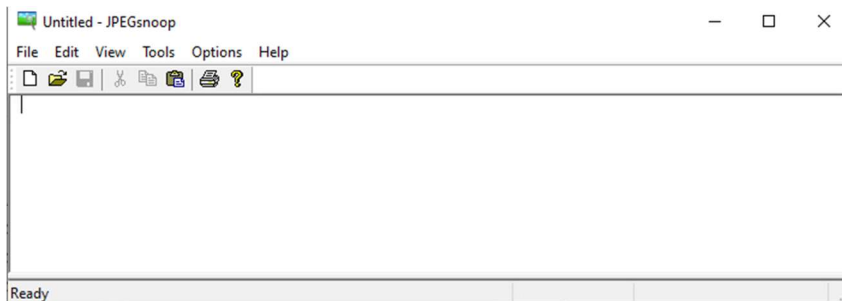


```
start .\cover.txt:snoop.exe
```



```
mklink doit.exe cover.txt:snoop.exe
```

```
start doit.exe
```



## Step 2:

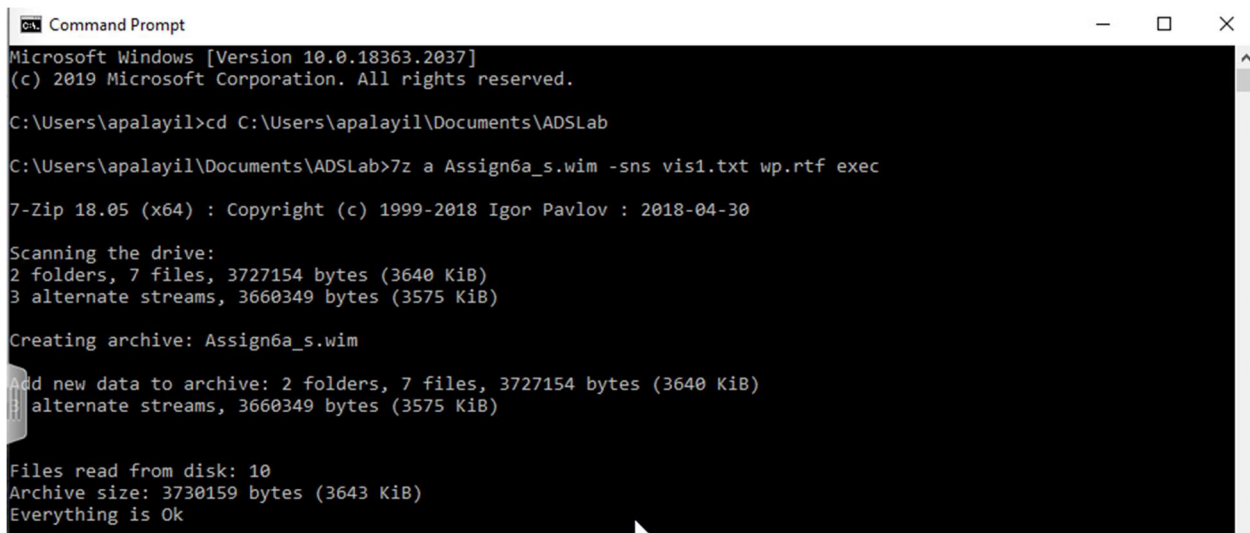
Using the resources in the ‘Alternate Data Streams’ there are various ways to send a file with the maintenance of the ADS. To send the files across the internet with the ADS intact, you can use a file compression tool like 7-Zip and the command line tool SysInternals Streams. To send the files

to a non-NTFS system and keep the ADS intact, you can use a file archiver like 7-Zip. This will ensure that the ADS is included in the archive. Using the command prompt, 7z a Filename.wim command we can add files to the archive and using -sns switch the NTFS streaming is available. Similarly, this can be used to send the file across the internet with the ADS intact. When the recipient receives the archive, they can extract the files and the ADS will be intact.

### Step 3:

We add a 7z.exe file to the ADSLab folder to execute 7z in the command prompt. In the command prompt where we are already in the ADS directory, We run the following command:

```
7z a Assign6a.wim -sns vis1.txt wp.rtf exec
```



```
Command Prompt
Microsoft Windows [Version 10.0.18363.2037]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\apalayil>cd C:\Users\apalayil\Documents\ADSLab
C:\Users\apalayil\Documents\ADSLab>7z a Assign6a_s.wim -sns vis1.txt wp.rtf exec

7-Zip 18.05 (x64) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30

Scanning the drive:
2 folders, 7 files, 3727154 bytes (3640 KiB)
3 alternate streams, 3660349 bytes (3575 KiB)

Creating archive: Assign6a_s.wim
Add new data to archive: 2 folders, 7 files, 3727154 bytes (3640 KiB)
3 alternate streams, 3660349 bytes (3575 KiB)

Files read from disk: 10
Archive size: 3730159 bytes (3643 KiB)
Everything is Ok
```

### Conclusion:

After following through the Complete Lecture of Alternate Data Streams from the resources, I was able to understand how ADS works within files and folders and how to send files with the ADS intact.