

## Anti-Forensics

In this lab you will use a number of tools/methods to perform data hiding and data modifications.

By the end of the lab you will be able to

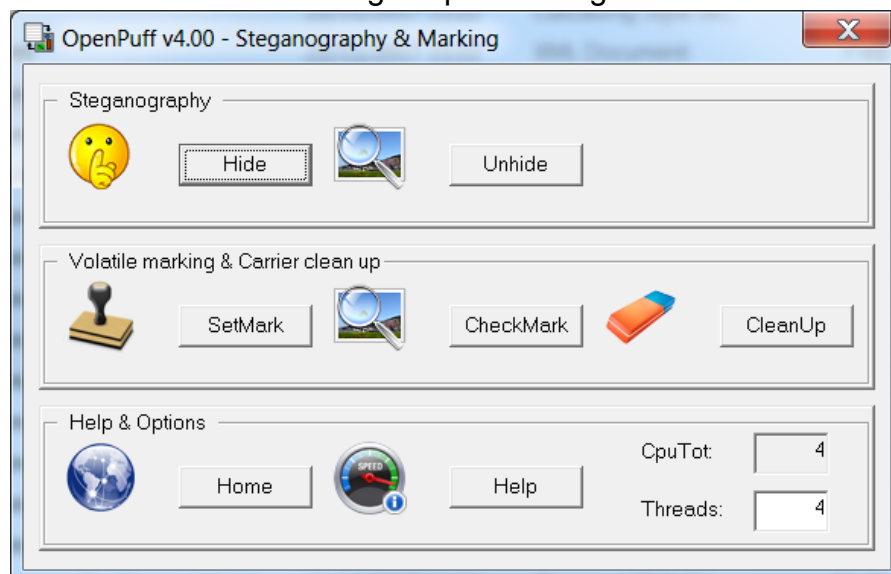
- A. Understand the impact of anti-forensic tools/methods upon digital forensic investigations
- B. Use OpenPuff to hide and recover hidden messages
- C. Use Alternate Data Streams (ADS) to hide information on an NTFS system
- D. Use Bulk Rename utility to modify file's attributes

### Task 1

In this task, you need to use OpenPuff to hide and retrieve hidden information. OpenPuff is a steganography tool with a range of functionality including using a **decoy**. It can be downloaded from moodle or from the following link [https://download.cnet.com/OpenPuff/3000-2092\\_4-75450743.html](https://download.cnet.com/OpenPuff/3000-2092_4-75450743.html)

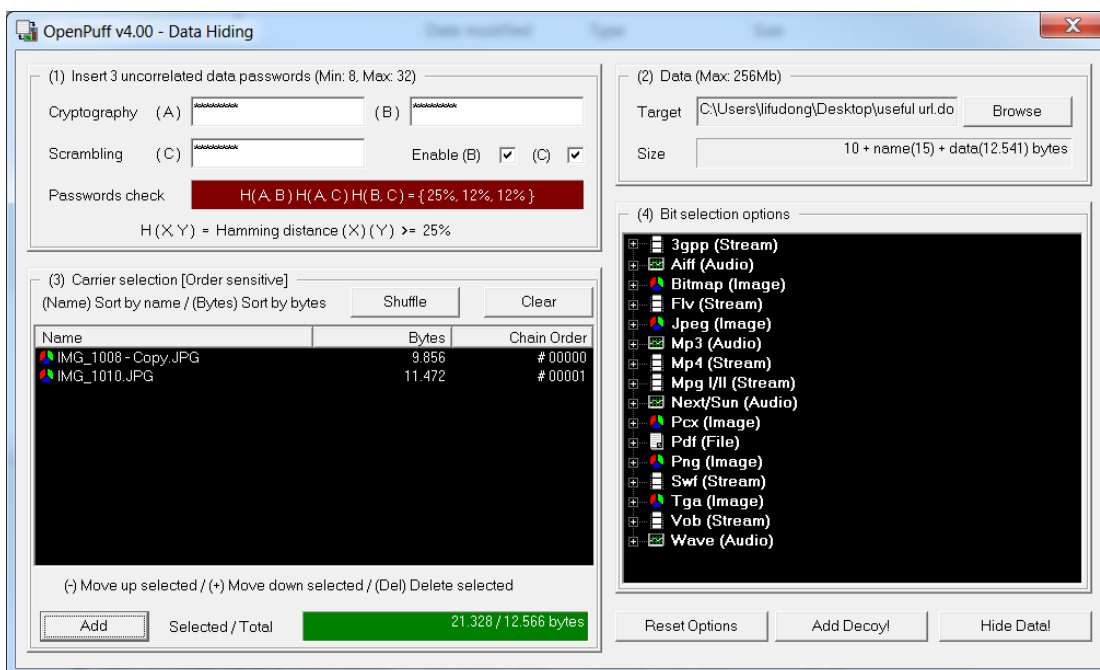
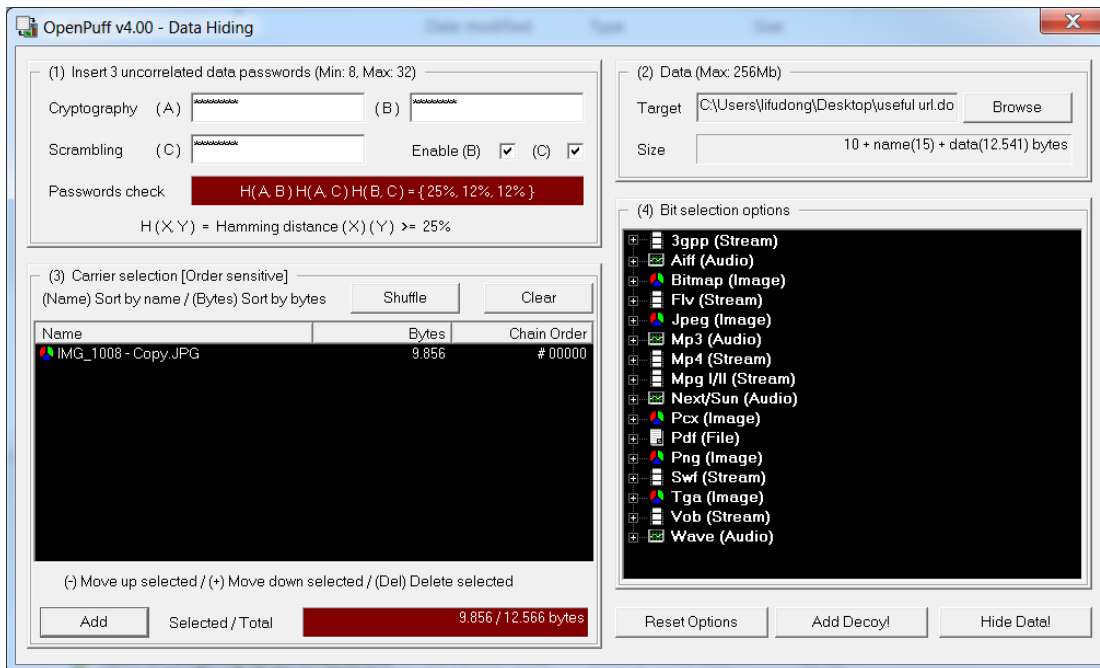
#### Part 1:

Once you open the OpenPuff application, you can do various things, including hiding information and embedding simple message.

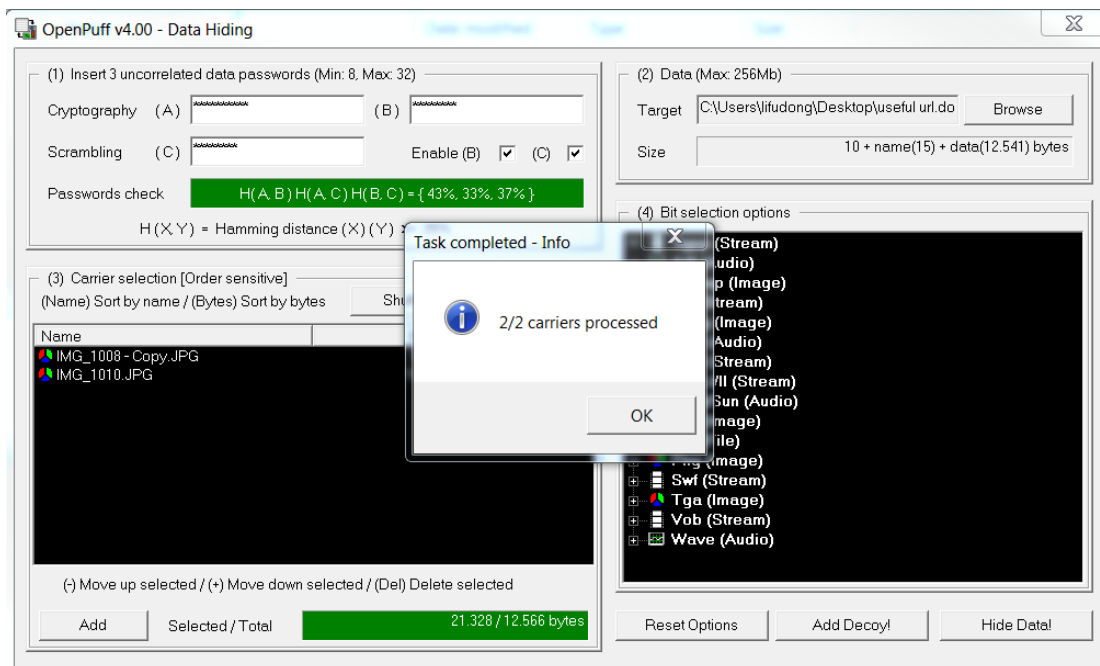
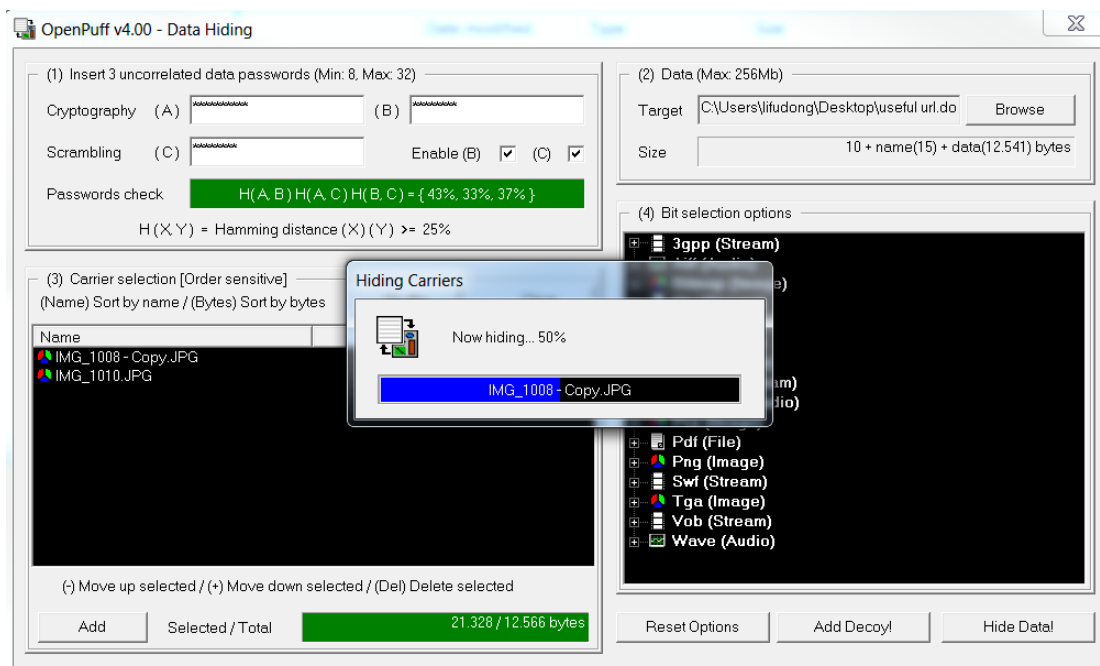


To hide the information, click on the “Hide” button and follow the instructions provided by the tool

1. Choose 3 uncorrelated data passwords [**make sure you remember them**]
2. Choose the file that needs to be stegged
3. Choose a carrier file. More carrier files may be required (as shown in the following figures); what are the pros and cons of using multiple carriers?
4. Choose a bit selection option and remember it (**you will need it for the Unhide process**)



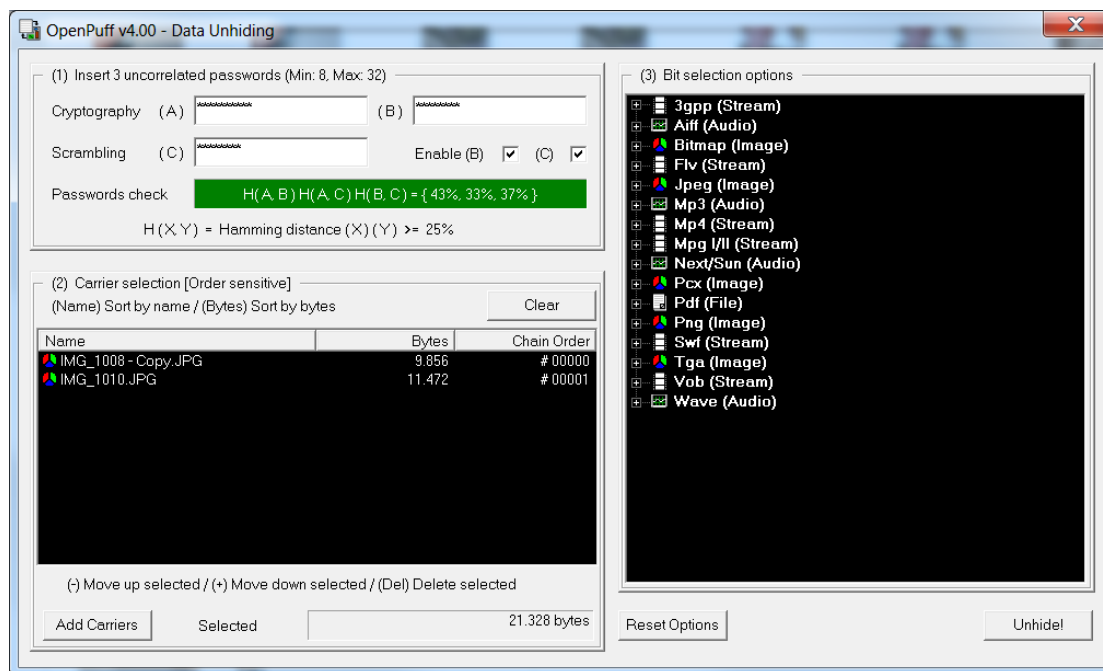
The hiding process may take some time; so be patient ☺



Once you complete the hiding process, note the difference between the new file and the original file (i.e. the carrier file).

To unhide the information, click on the “Unhide” button within the main interface and follow the instructions provided by the tool

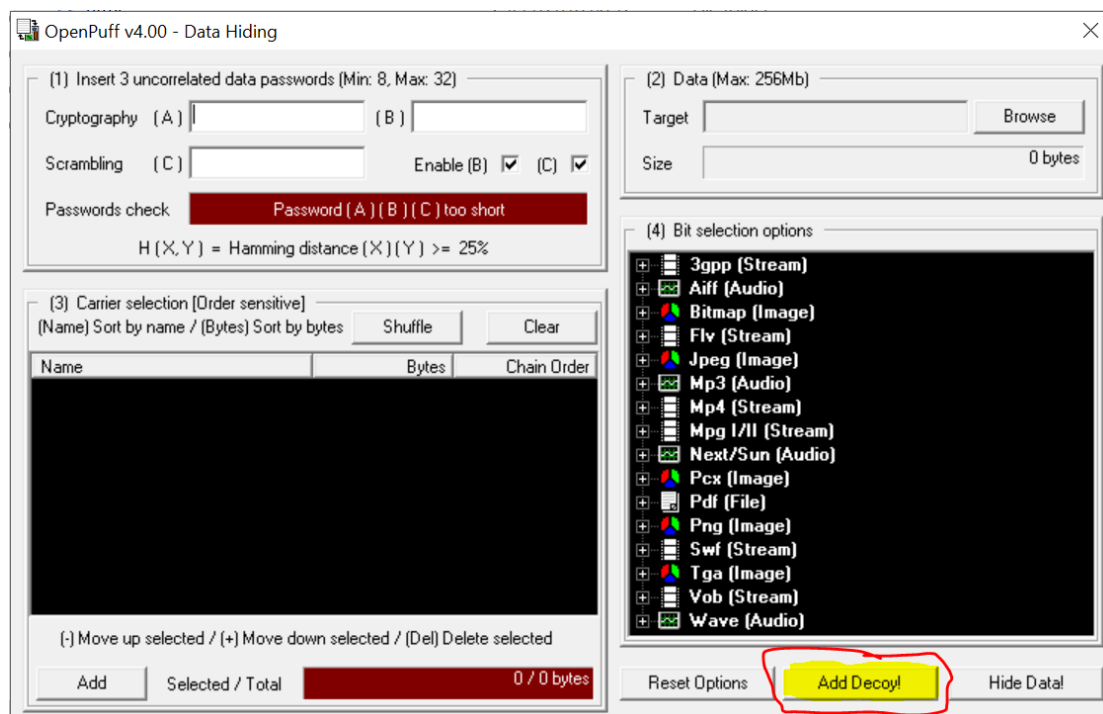
1. Insert the 3 passwords (if you can still remember them)
2. Select the carrier file(s)
3. Make sure an appropriate bit selection option is selected (or you can try other option and see what happens!)



Write down the things that you learned from this exercise.

## Part 2:

Repeat the part 1's process on a new image by adding a **decoy** and see what happens.

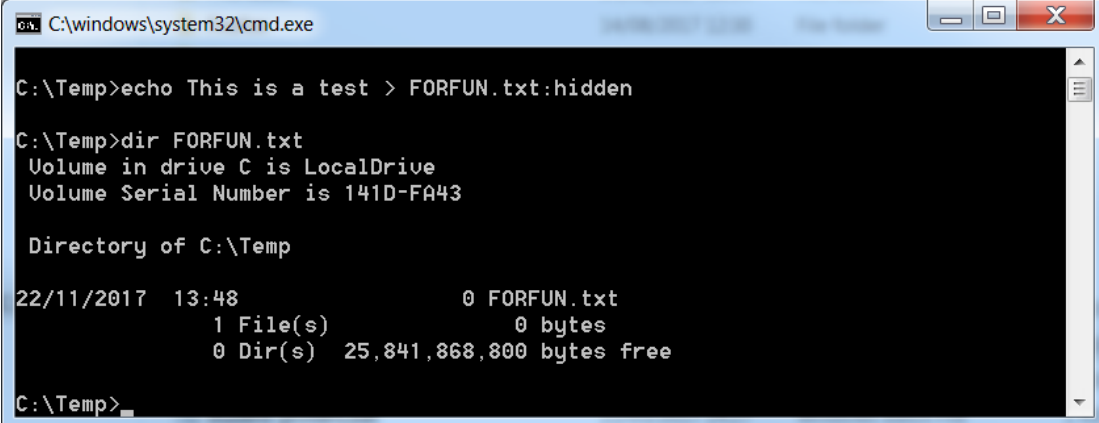


## Task 2

In this task, you need to use ADS to hide information. ADS allows arbitrary metadata to be associated with files and directories on Windows NTFS.

### Step 1: Creating an Alternate Data Stream

As an example, a string is written into an ADS named *hidden*, which is associated with file FORFUN.txt



```
C:\windows\system32\cmd.exe

C:\Temp>echo This is a test > FORFUN.txt:hidden

C:\Temp>dir FORFUN.txt
Volume in drive C is LocalDrive
Volume Serial Number is 141D-FA43

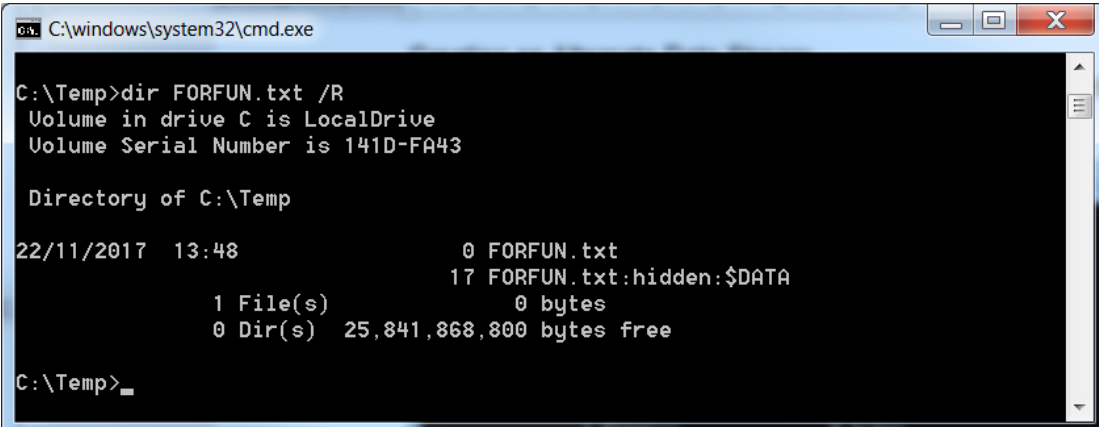
Directory of C:\Temp

22/11/2017  13:48                0 FORFUN.txt
               1 File(s)                0 bytes
               0 Dir(s) 25,841,868,800 bytes free

C:\Temp>
```

### Step 2: Listing files with Alternative Data Streams

On windows Vista and later, a list of alternate data streams can be obtained using “DIR /R”



```
C:\windows\system32\cmd.exe

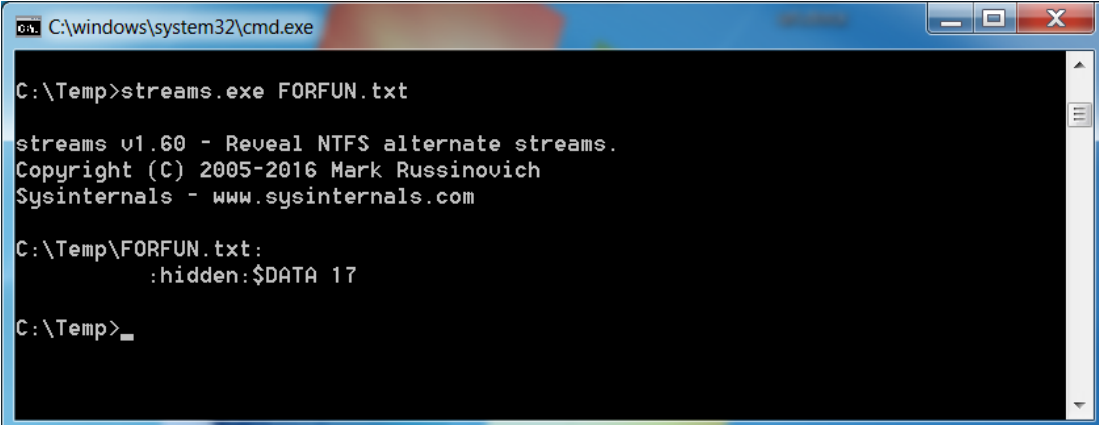
C:\Temp>dir FORFUN.txt /R
Volume in drive C is LocalDrive
Volume Serial Number is 141D-FA43

Directory of C:\Temp

22/11/2017  13:48                0 FORFUN.txt
                  17 FORFUN.txt:hidden:$DATA
               1 File(s)                0 bytes
               0 Dir(s) 25,841,868,800 bytes free

C:\Temp>
```

Alternatively, the SysInternals utility “Streams” can be used as demonstrated below. The Streams can be downloaded via the following link: <https://docs.microsoft.com/en-us/sysinternals/downloads/streams>



```
C:\windows\system32\cmd.exe

C:\Temp>streams.exe FORFUN.txt

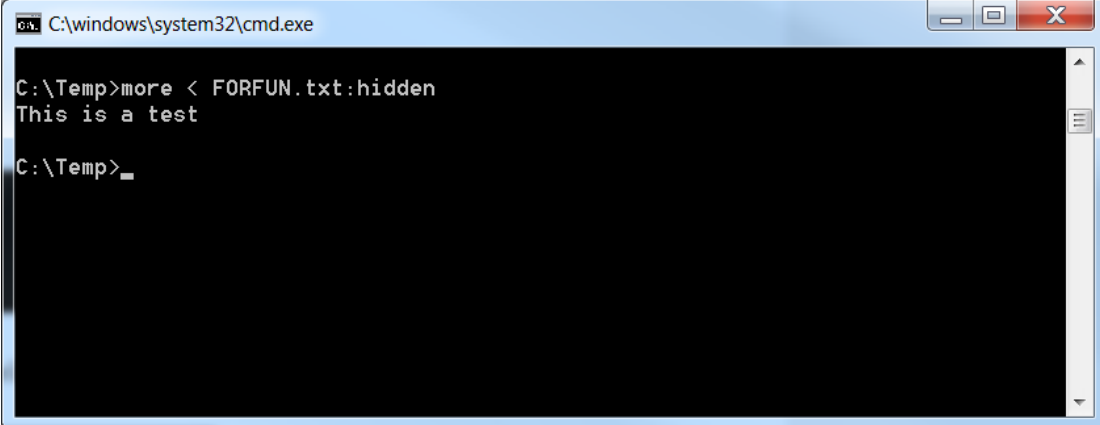
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Temp\FORFUN.txt:
      :hidden:$DATA 17

C:\Temp>
```

### Step 3: Review the hidden message

Once the hidden data is identified, the metadata can be viewed by redirecting from it to more



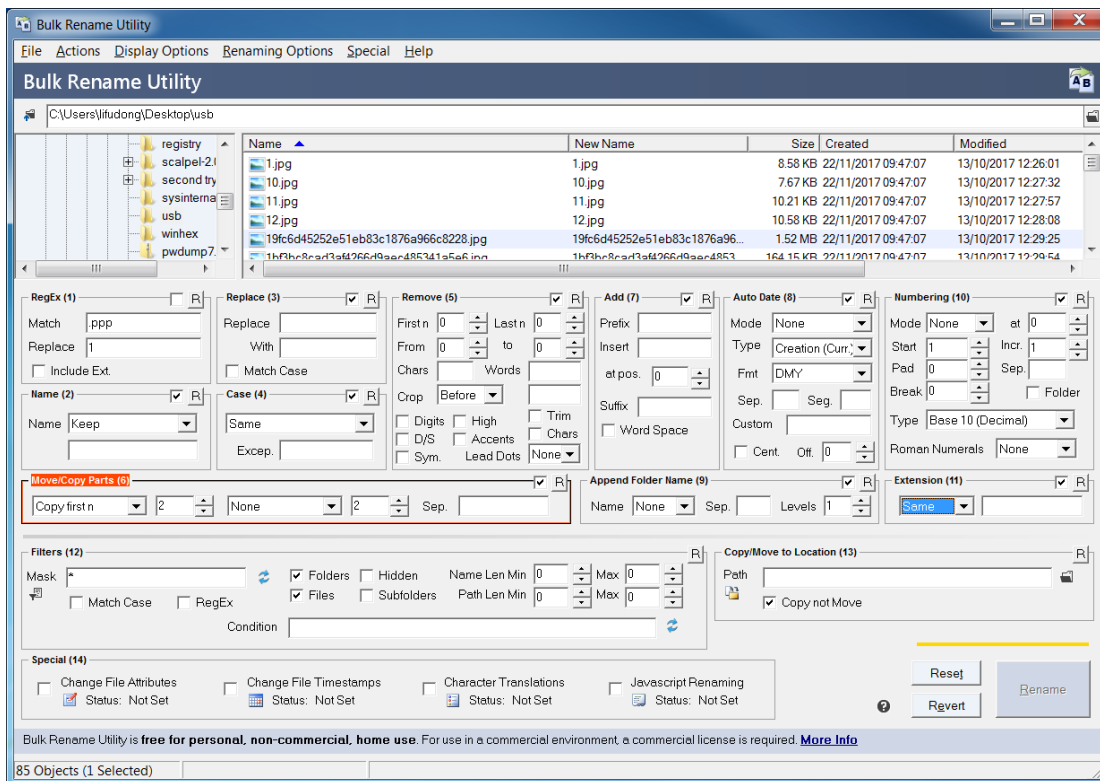
```
C:\windows\system32\cmd.exe
C:\Temp>more < FORFUN.txt:hidden
This is a test
C:\Temp>
```

Step 4: Once you understand how ADS works, test the method on several files. Also check the MD5 and SHA1 hash values of those files both with and without the ADS being put in place.

### Task 3

In this task, you need to use Bulk Rename Utility to modify various file attributes. The software can be downloaded from moodle or via the following link <https://www.bulkrenameutility.co.uk/Download.php>; also have a look at the manual pdf file if you have free time.

Once the Bulk Rename Utility is installed, you can modify different file metadata as shown below



Try each of the 14 options and observe the result.