Data Hiding Techniques

Using Tools Build Right Into Windows

Prashant Mahajan

Dedicated to Indranil Yadav

07/08/1989 – 05/02/2008

What is Data Hiding ?

- Data Hiding is a very ancient art.
  - Caesar cipher.
  - Egyptians used symbolic language in their pyramids.
  - Coded Language.
  - Writing with invisible ink.

- With the dawn of the Digital World, now just the methods have changed, but the **aim** is still the same.

What is Data Hiding ? Cont.

- In Modern Times, Data Hiding is associated with digital forms such as *cryptography, steganography*, and *watermarking*.
  - *Cryptography* is obscuring the content of the message, but not the communication of the message.
  - *Steganography, which is greek for "covered writing"*, is hiding the very communication of the message.
  - *Watermarking* attempts to add sufficient metadata to a message to establish ownership, provenance, source, etc.

- But, it is much more than that.

Reasons Behind Hiding Data

- Personal, Private Data.
- Sensitive Data.
- Confidential Data, Trade Secrets.
- To avoid Misuse of Data.
- Unintentional damage to data, human error, accidental deletion.
- Monetary, Blackmail Purposes.
- Hide Traces of a crime.
- For Fun. ☺

Overview

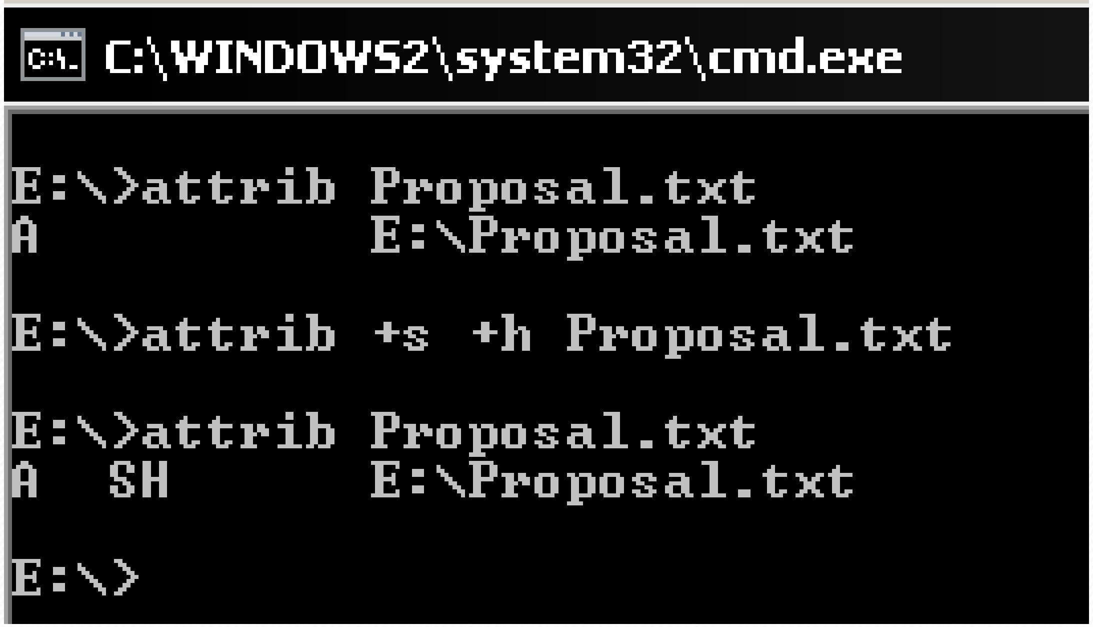
- Basic Logical Techniques used to Hide Data in Microsoft Windows XP.
- Thinking out of the box, using applications for things other than their intended use.
- Data Hiding using internal concept of Microsoft Windows XP.
- A dive into the File System of Microsoft Windows XP, i.e. NTFS.

Logical Techniques

Logical Techniques

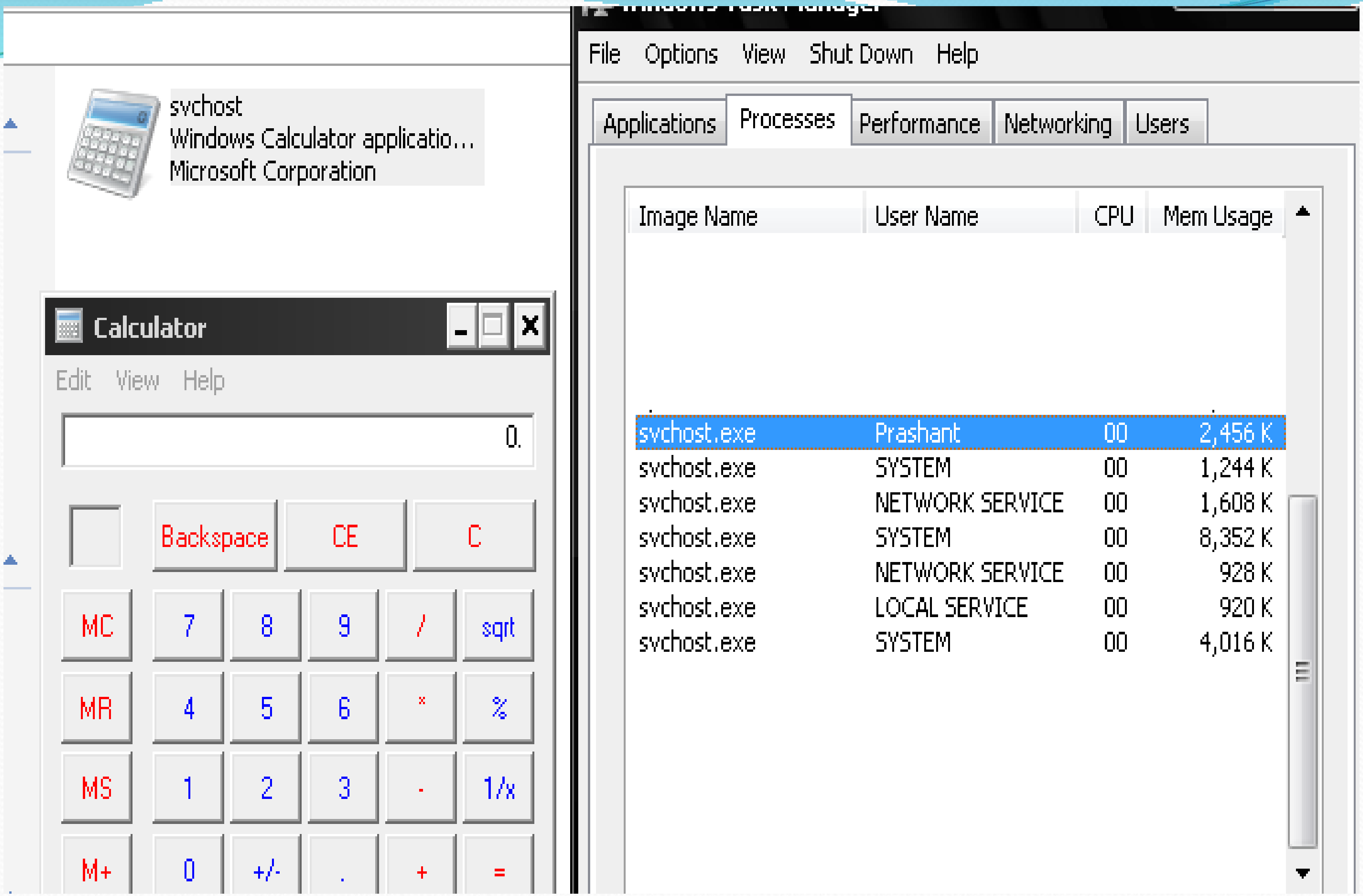
- The Usual right click and hide; the hidden attribute.
- Assign the file a system attribute.
- Rename it as a system file and paste it in the windows directory.
    - Most often used by Malware
        - Svchost.exe
- Change of extension.
- Change of Icon.
- Rename as “null”.

Assigning the Hidden and System Attribute



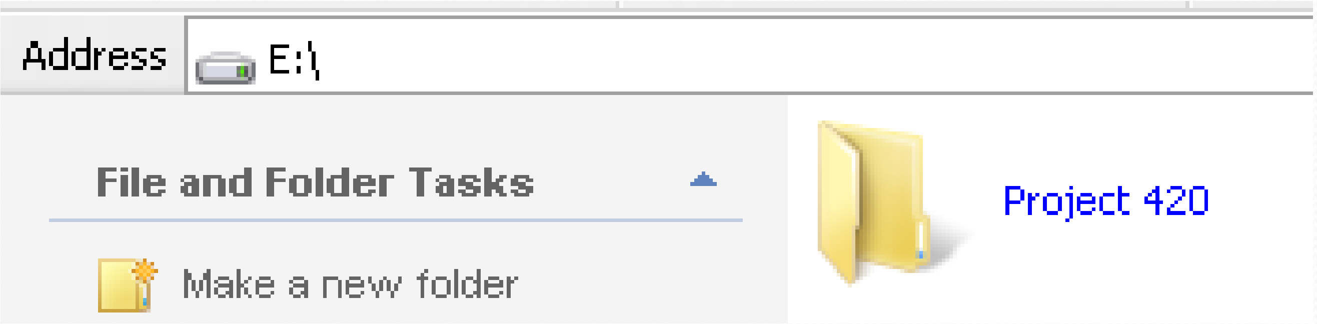
C:\WINDOWS2\system32\cmd.exe

```
E:\>attrib Proposal.txt
A            E:\Proposal.txt

E:\>attrib +s +h Proposal.txt

E:\>attrib Proposal.txt
A   SH       E:\Proposal.txt

E:\>
```

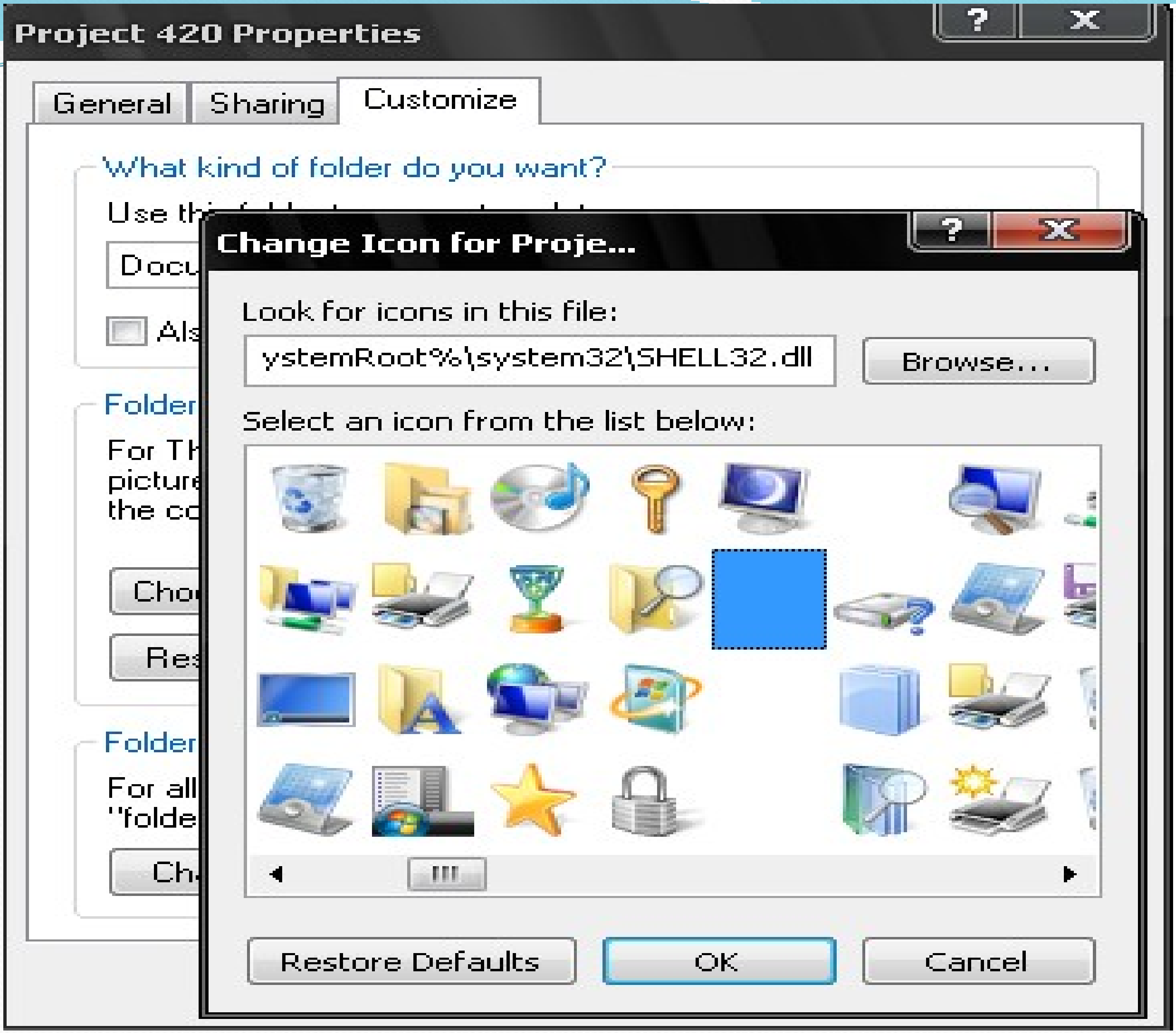


svchost
Windows Calculator applicatio…
Microsoft Corporation

Image Name	User Name	CPU	Mem Usage
svchost.exe	Prashant	00	2,456 K
svchost.exe	SYSTEM	00	1,244 K
svchost.exe	NETWORK SERVICE	00	1,608 K
svchost.exe	SYSTEM	00	8,352 K
svchost.exe	NETWORK SERVICE	00	928 K
svchost.exe	LOCAL SERVICE	00	920 K
svchost.exe	SYSTEM	00	4,016 K



Address E:\



Project 420 Properties

What kind of folder do you want?

Use thi

Docu

□ Als

Folder

For Th
picture
the co

Folder

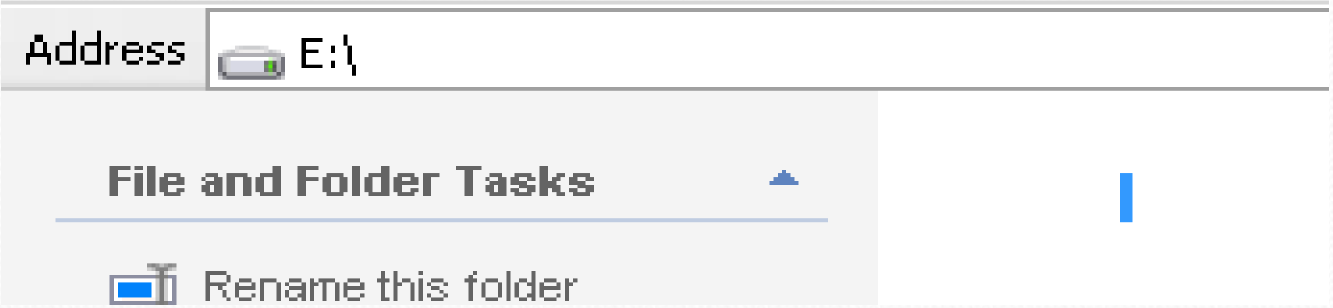
For all
"folde

Change Icon for Proje...

Look for icons in this file:

ystemRoot%\system32\SHELL32.dll

Select an icon from the list below:



Address E:\

Think Out of the Box

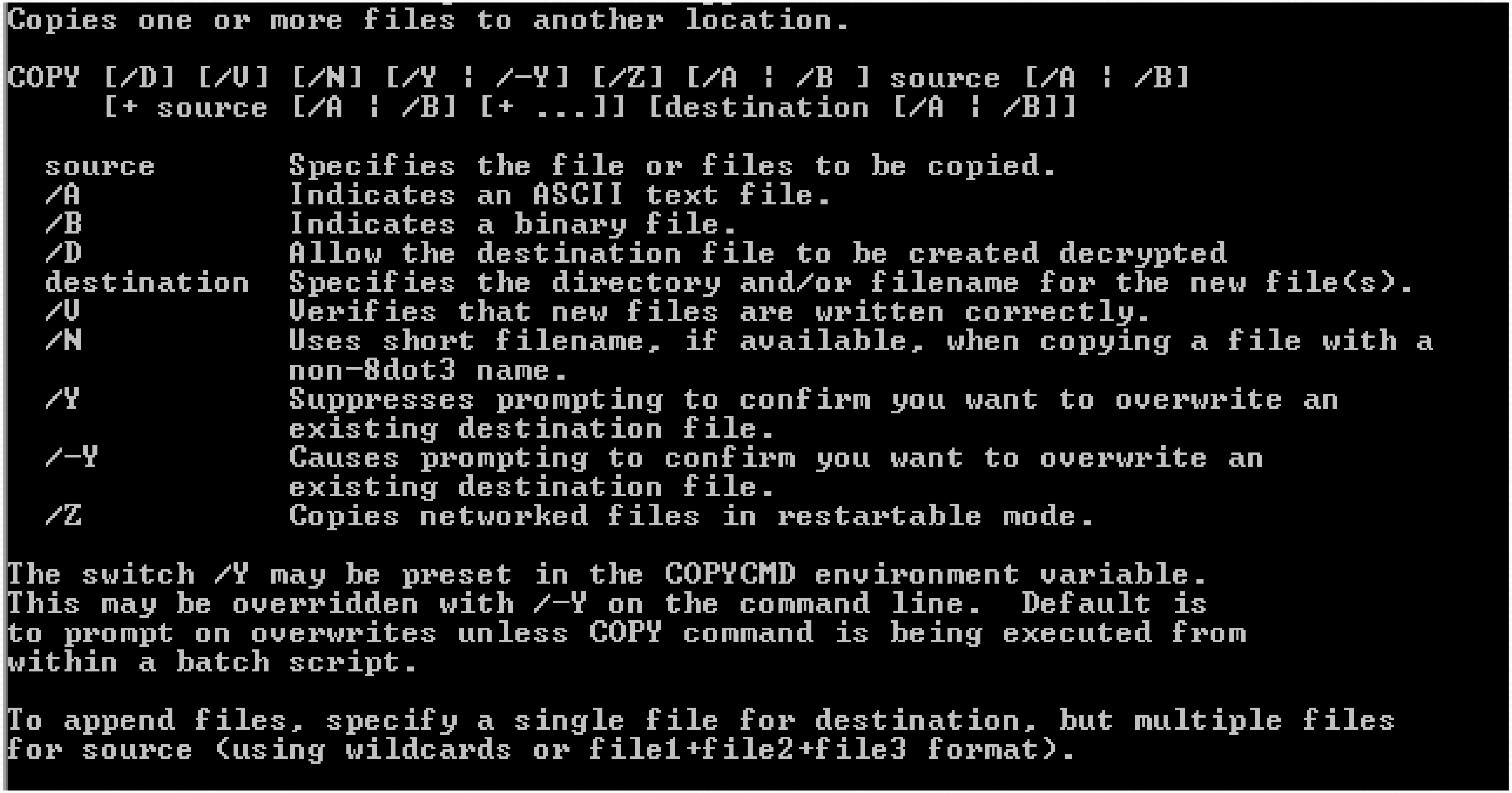
It is often said, if you want to catch a criminal, first learn to think like one. Therefore, to catch a Hacker, learn to

Think Out of the Box.

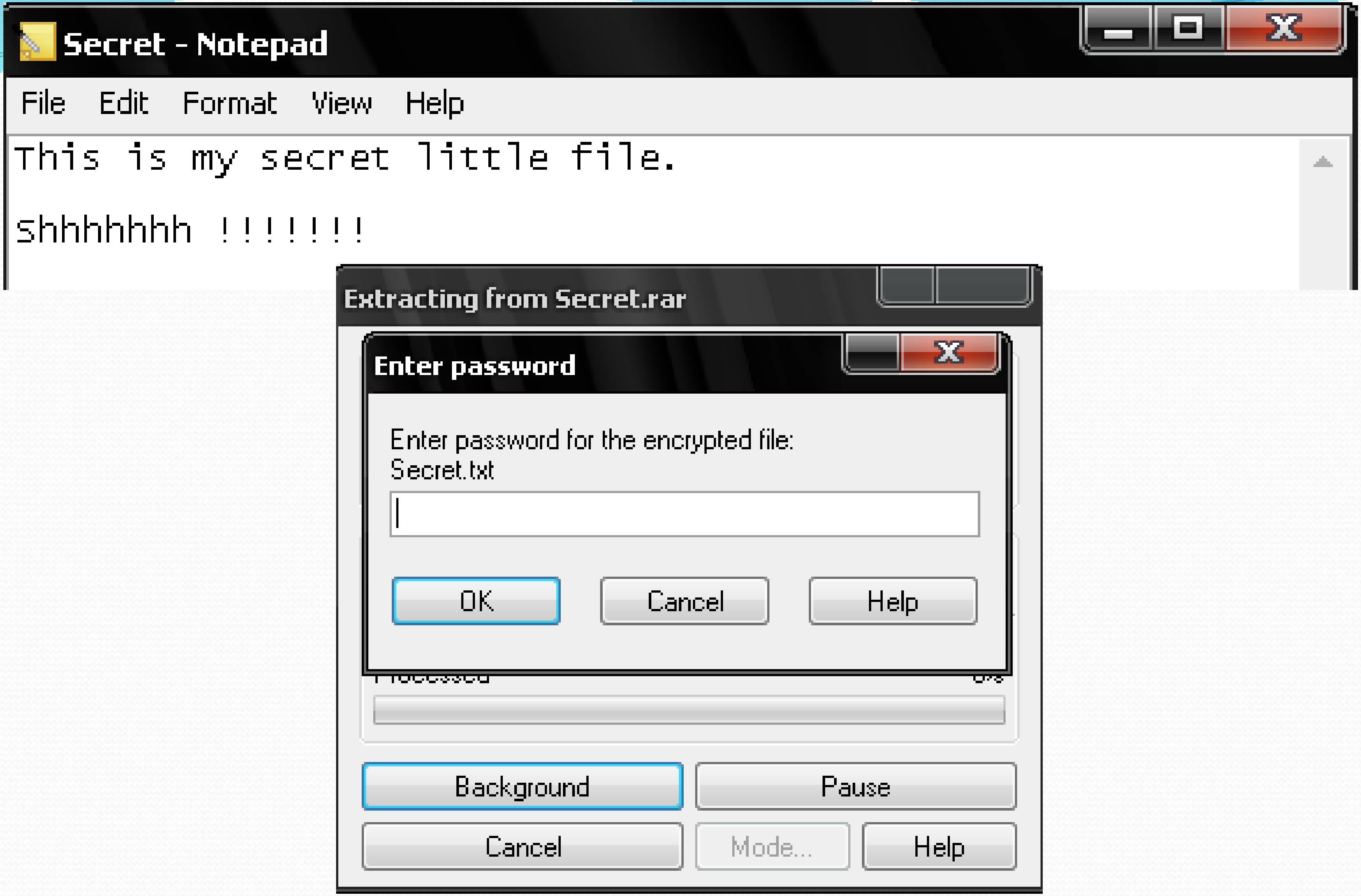
The Copy Command

- What’s the use of the “copy” command, from DOS (Disk Operating System).
    - To make a copy of a file.
    - To copy one file from one location to another.
    - To copy multiple files to a specified folder.
    - And ?

Well, Guess what, Hide Your Data !



```
Copies one or more files to another location.

COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/A | /B ] source [/A | /B]
     [+ source [/A | /B] [+ ...]] [destination [/A | /B]]

  source       Specifies the file or files to be copied.
  /A           Indicates an ASCII text file.
  /B           Indicates a binary file.
  /D           Allow the destination file to be created decrypted
  destination  Specifies the directory and/or filename for the new file(s).
  /V           Verifies that new files are written correctly.
  /N           Uses short filename, if available, when copying a file with a
               non-8dot3 name.
  /Y           Suppresses prompting to confirm you want to overwrite an
               existing destination file.
  /-Y          Causes prompting to confirm you want to overwrite an
               existing destination file.
  /Z           Copies networked files in restartable mode.

The switch /Y may be preset in the COPYCMD environment variable.
This may be overridden with /-Y on the command line.  Default is
to prompt on overwrites unless COPY command is being executed from
within a batch script.

To append files, specify a single file for destination, but multiple files
for source (using wildcards or file1+file2+file3 format).
```



Secret - Notepad

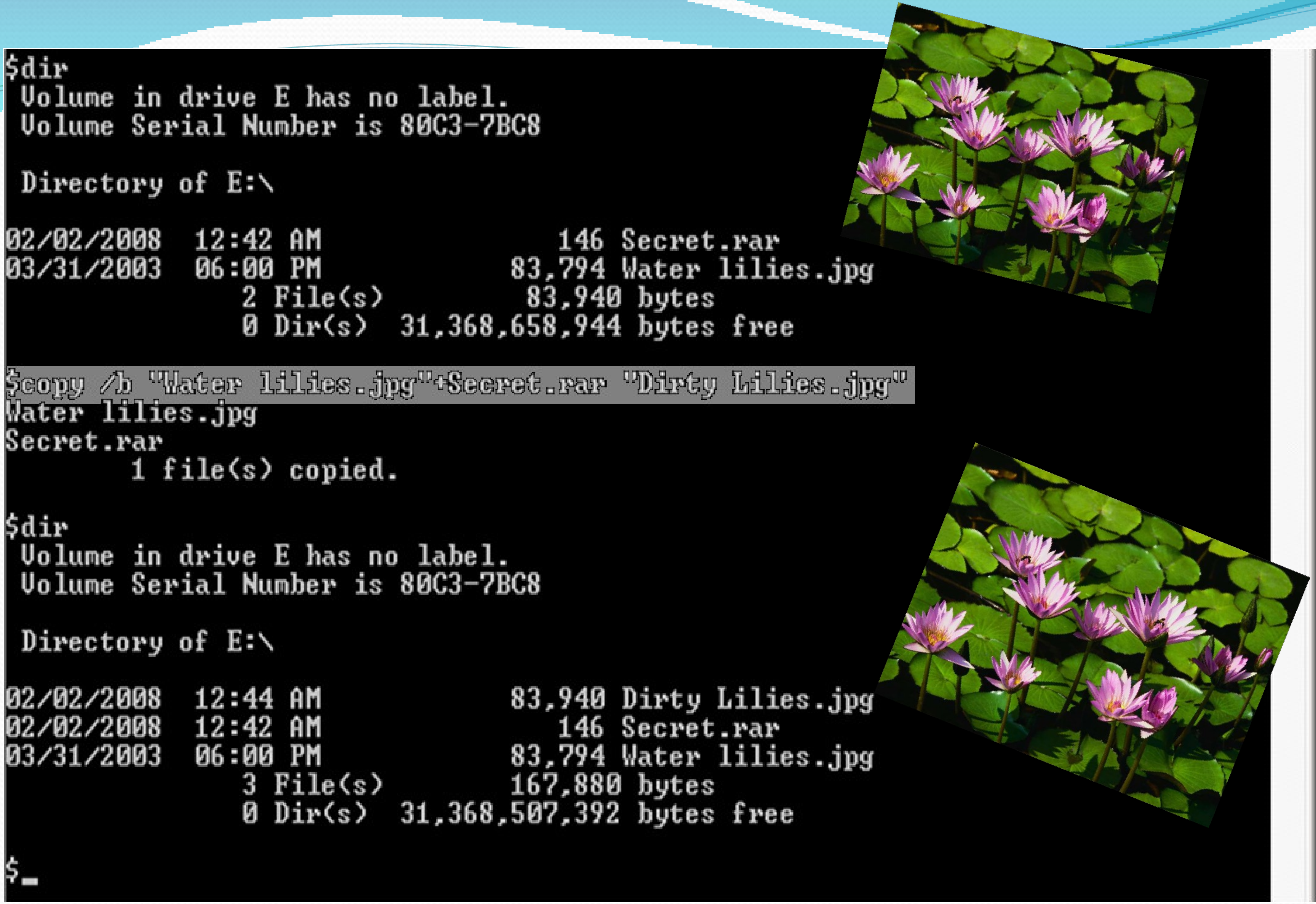
This is my secret little file.

shhhhhhh !!!!!!!

Extracting from Secret.rar

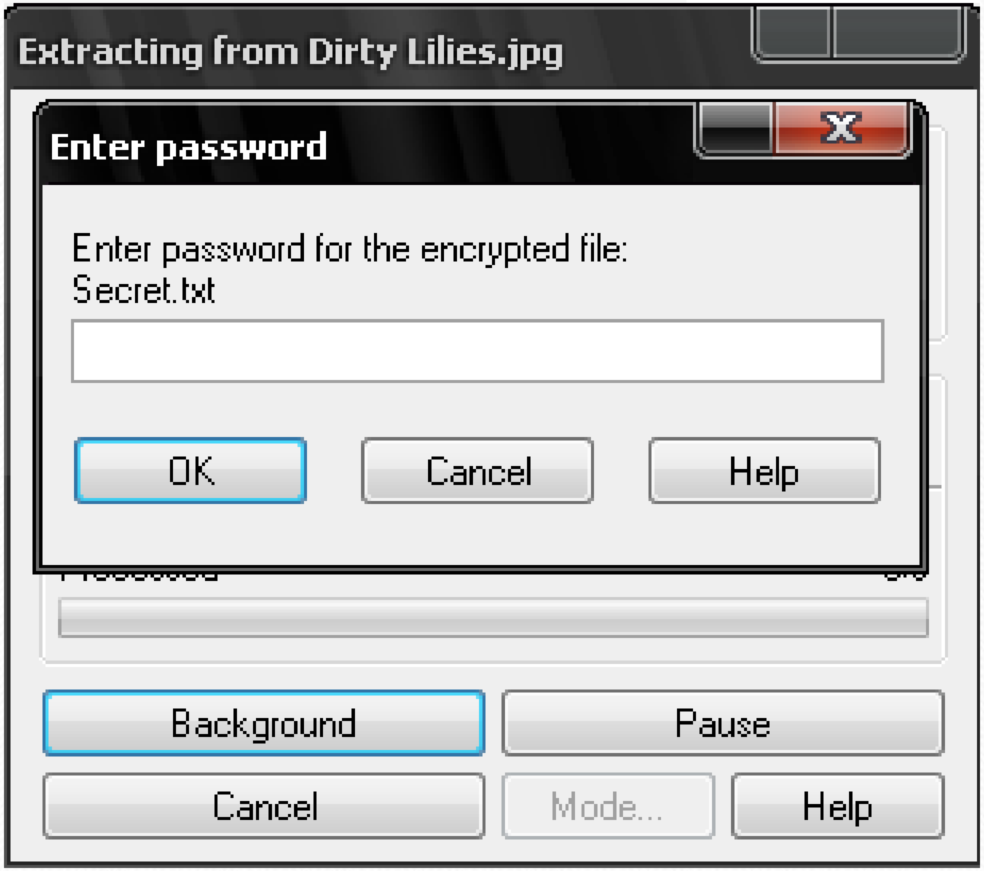
Enter password

Enter password for the encrypted file:
Secret.txt



```
$dir
 Volume in drive E has no label.
 Volume Serial Number is 80C3-7BC8

 Directory of E:\

02/02/2008  12:42 AM                   146 Secret.rar
03/31/2003  06:00 PM                83,794 Water lilies.jpg
               2 File(s)             83,940 bytes
               0 Dir(s)  31,368,658,944 bytes free

$copy /b "Water lilies.jpg"+Secret.rar "Dirty Lilies.jpg"
Water lilies.jpg
Secret.rar
        1 file(s) copied.

$dir
 Volume in drive E has no label.
 Volume Serial Number is 80C3-7BC8

 Directory of E:\

02/02/2008  12:44 AM                83,940 Dirty Lilies.jpg
02/02/2008  12:42 AM                   146 Secret.rar
03/31/2003  06:00 PM                83,794 Water lilies.jpg
               3 File(s)            167,880 bytes
               0 Dir(s)  31,368,507,392 bytes free

$_
```

Voila !!



Extracting from Dirty Lilies.jpg

Enter password

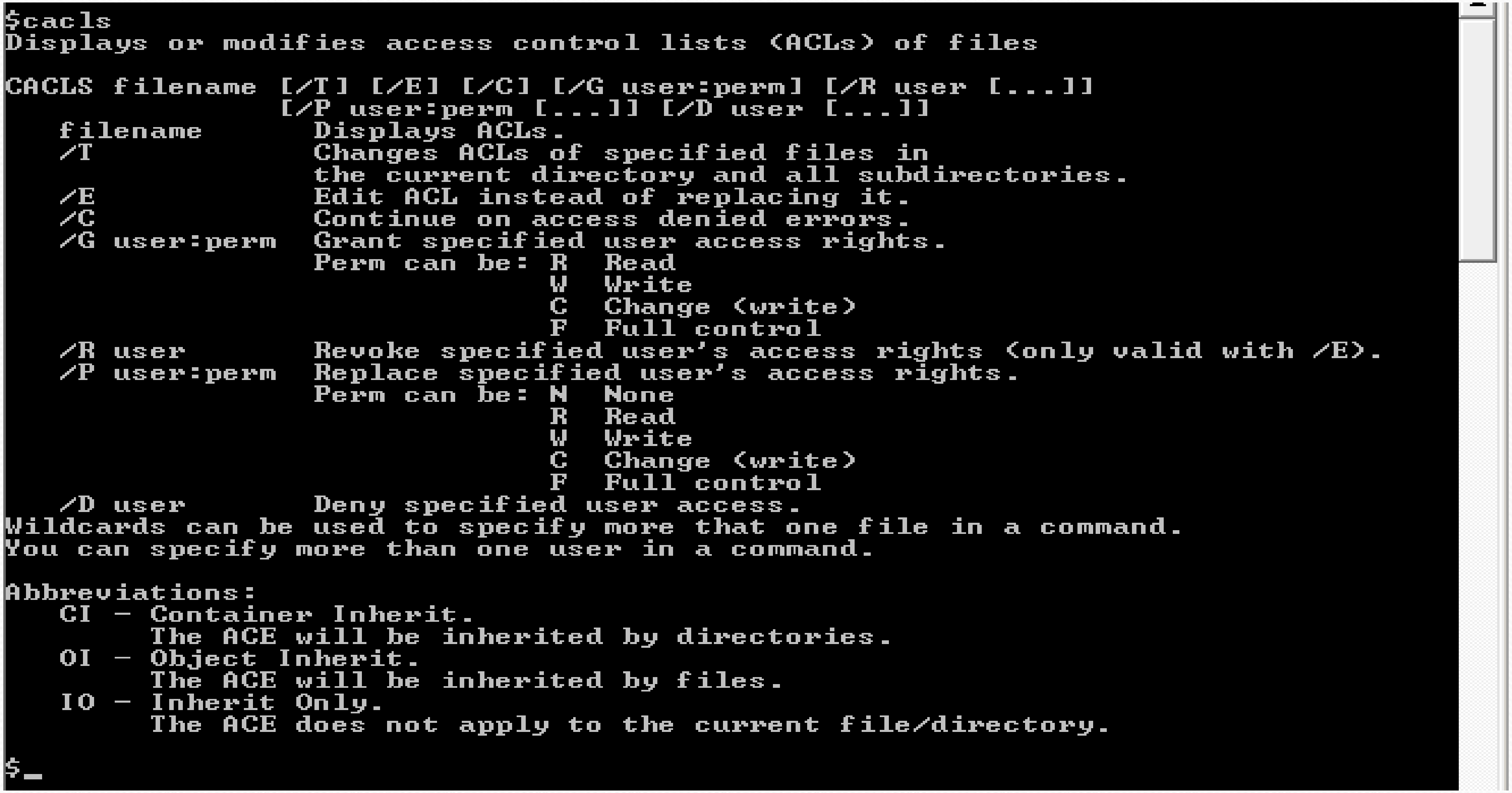
Enter password for the encrypted file:
Secret.txt

Access Denied

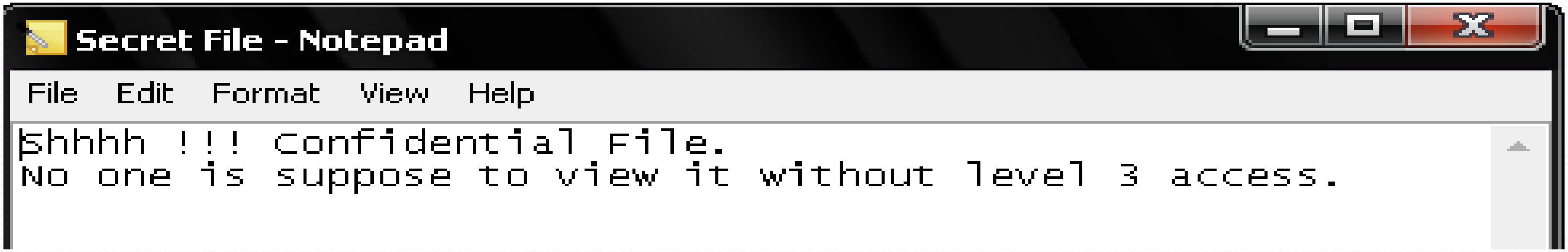
- To ***hide*** means to prevent from being seen or discovered.
- So, in the language of the computer;
    - Access Denied.
- You control the access to the file.
- And how do you control access in Microsoft Windows XP ?

Access Control Lists (ACLs)

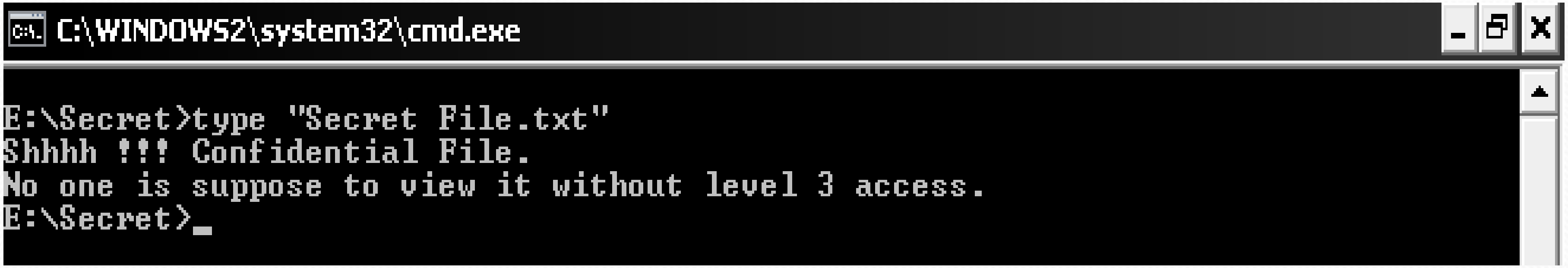
The Cacls Command



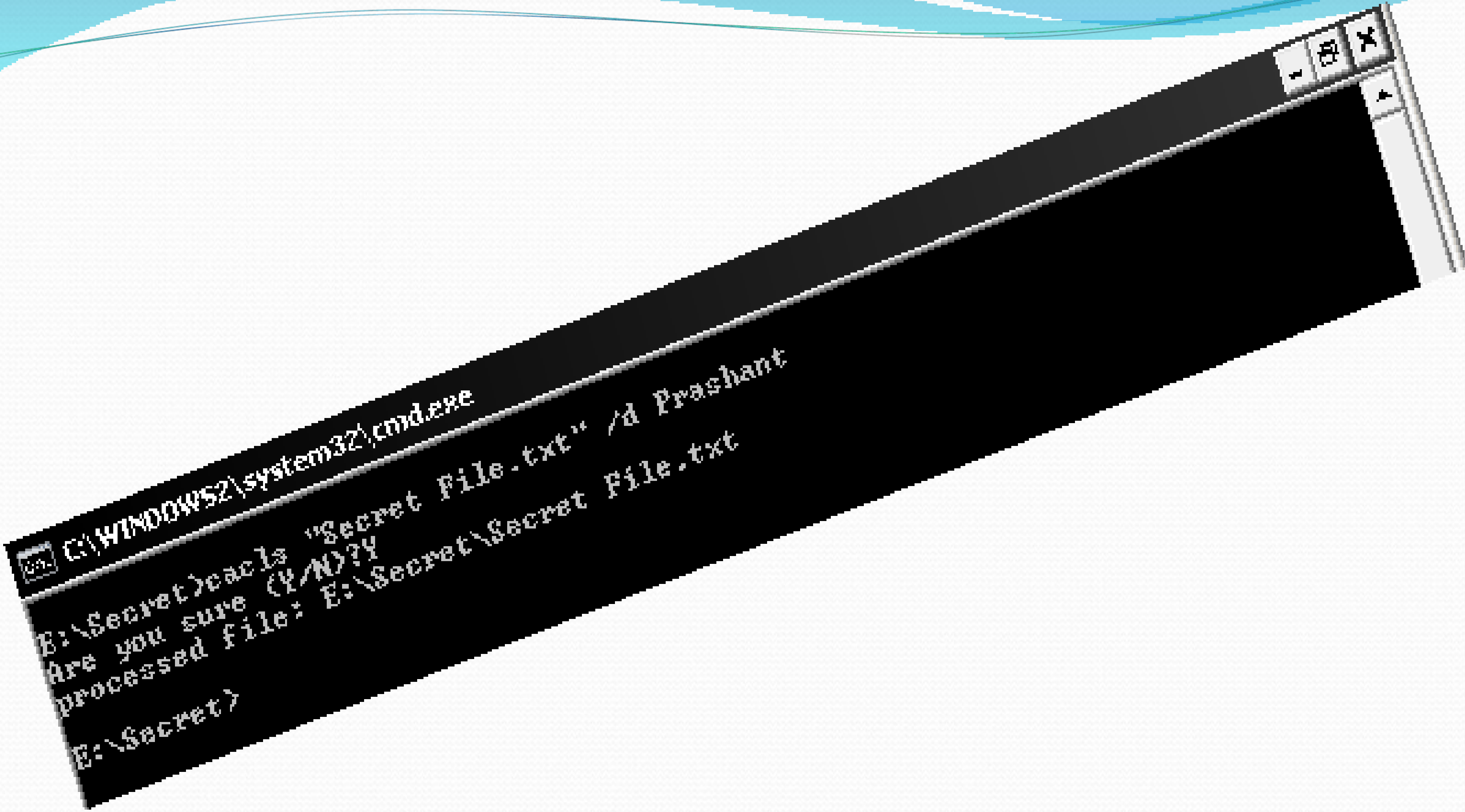
```
$cacls
Displays or modifies access control lists (ACLs) of files

CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]]
               [/P user:perm [...]] [/D user [...]]
   filename      Displays ACLs.
   /T            Changes ACLs of specified files in
                 the current directory and all subdirectories.
   /E            Edit ACL instead of replacing it.
   /C            Continue on access denied errors.
   /G user:perm  Grant specified user access rights.
                 Perm can be: R  Read
                              W  Write
                              C  Change (write)
                              F  Full control
   /R user       Revoke specified user's access rights (only valid with /E).
   /P user:perm  Replace specified user's access rights.
                 Perm can be: N  None
                              R  Read
                              W  Write
                              C  Change (write)
                              F  Full control
   /D user       Deny specified user access.
Wildcards can be used to specify more that one file in a command.
You can specify more than one user in a command.

Abbreviations:
   CI - Container Inherit.
        The ACE will be inherited by directories.
   OI - Object Inherit.
        The ACE will be inherited by files.
   IO - Inherit Only.
        The ACE does not apply to the current file/directory.

$_
```



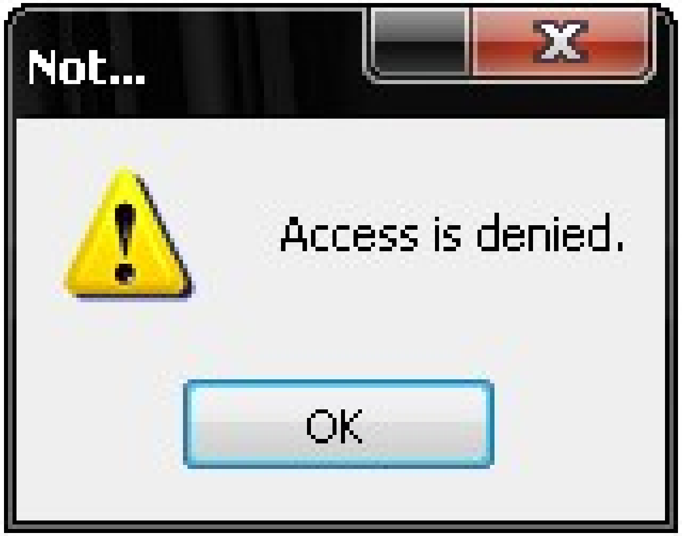
```
Shhhh !!! Confidential File.
No one is suppose to view it without level 3 access.
```



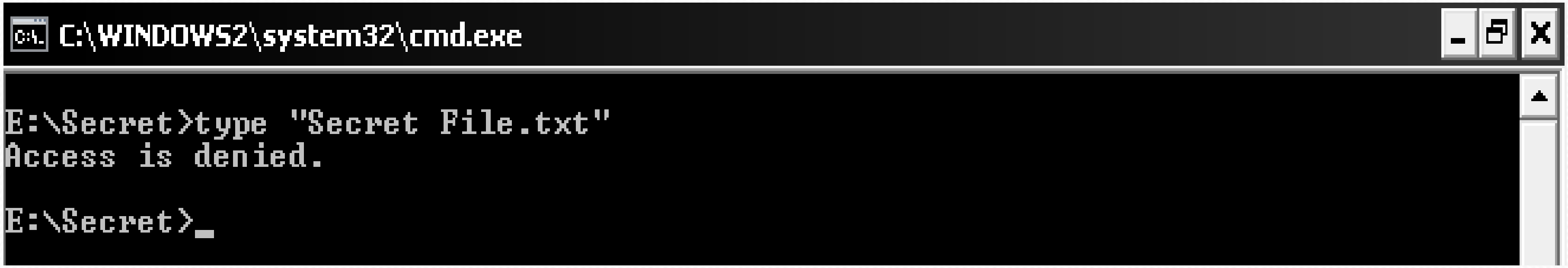
```
E:\Secret>type "Secret File.txt"
Shhhh !!! Confidential File.
No one is suppose to view it without level 3 access.
E:\Secret>_
```



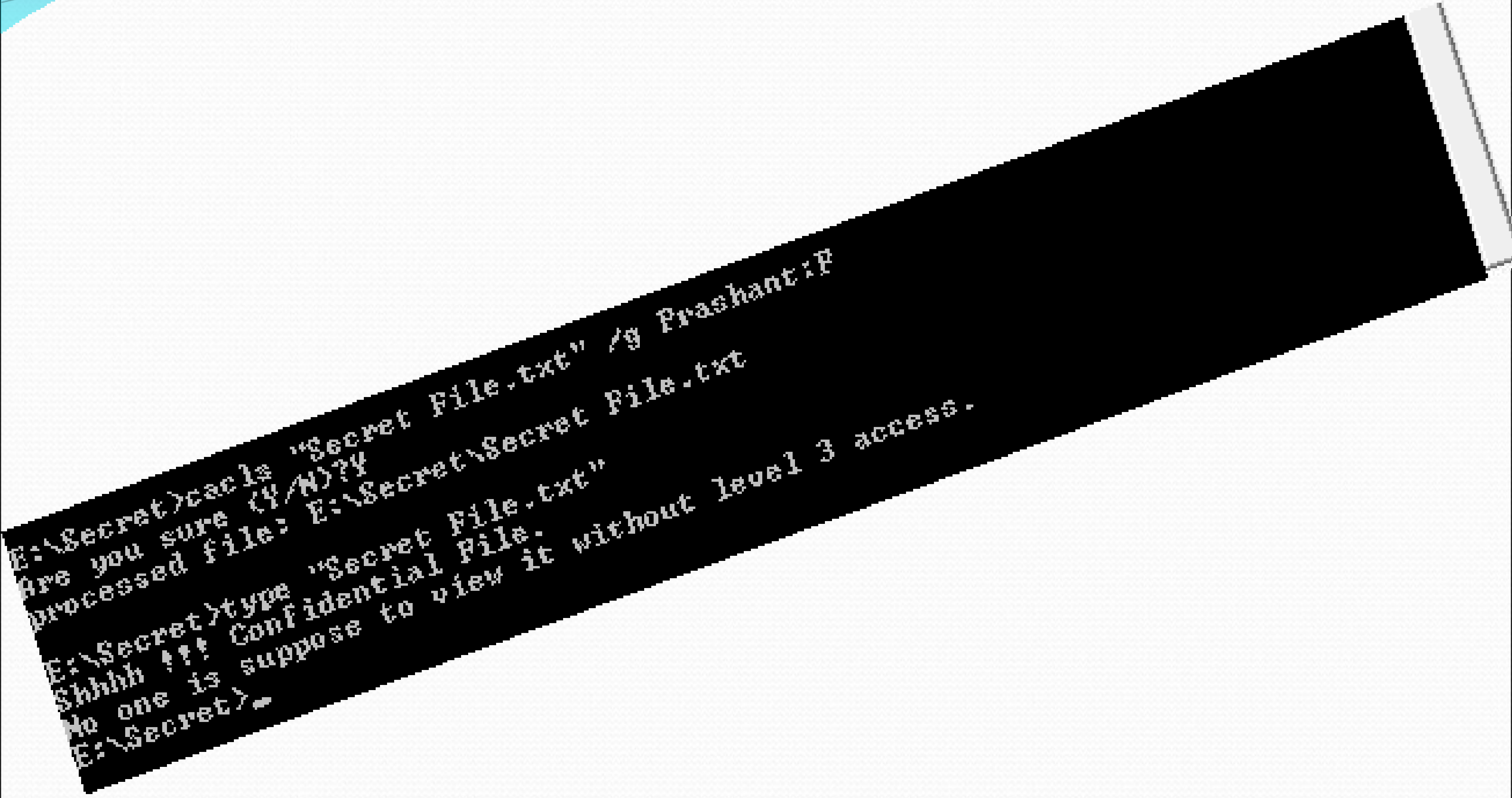
```
E:\Secret>cacls "Secret File.txt" /d Prashant
Are you sure (Y/N)?Y
processed file: E:\Secret\Secret File.txt

E:\Secret>
```



Access is denied.



```
E:\Secret>type "Secret File.txt"
Access is denied.

E:\Secret>_
```



```
E:\Secret>cacls "Secret File.txt" /g Prashant:P
Are you sure (Y/N)?y
processed file: E:\Secret\Secret File.txt

E:\Secret>type "Secret File.txt"
Shhhh !!! Confidential File.
No one is suppose to view it without level 3 access.
E:\Secret>
```

Internal Concept of Microsoft Windows XP

Crooks and Hooks of
CLSID

CLSID

- CLSID
  - A Class ID(CLSID) is a 128 bit (large) number that represents a unique id for a software application or application component.
- Its Use
  - They are used by Windows to identify software components without having to know their “name”. They can also be used by software applications to identify a computer, file or other item.
- Where do they come from
  - Microsoft provides a utility called GUIDGEN.exe that generates these numbers. They are generated by using the current time, network adapter address (if present) and other items in your computer so that no two numbers will ever be the same.

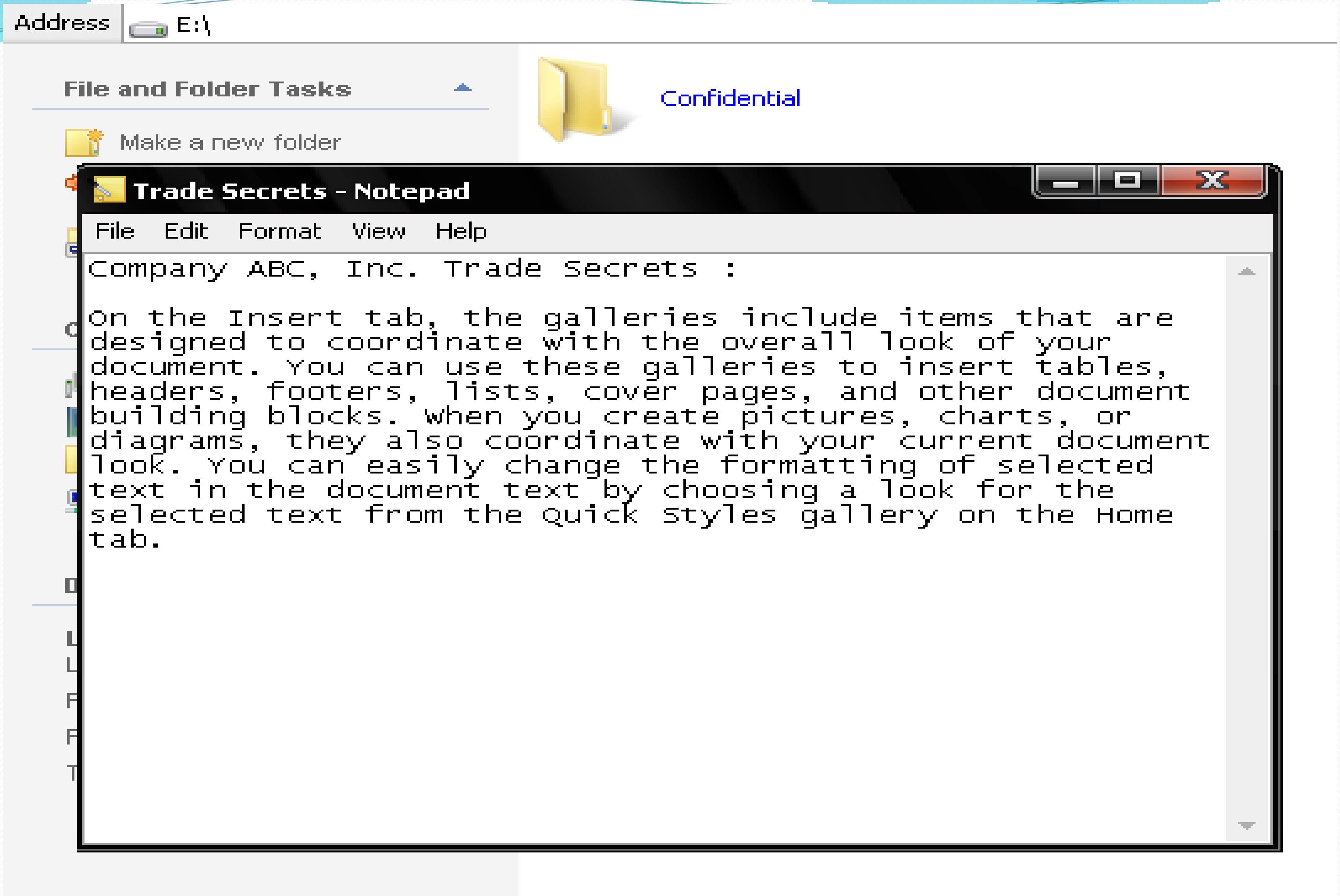
Certain special folders within the operating system are identified by unique strings.

CLSID	Meaning / Location
{48e7caab-b918-4e58-a94d-505519c795dc}	Start Menu Folder
{20d04fe0-3aea-1069-a2d8-08002b30309d}	My Computer
{645ff040-5081-101b-9f08-00aa002f954e}	Recycle Bin

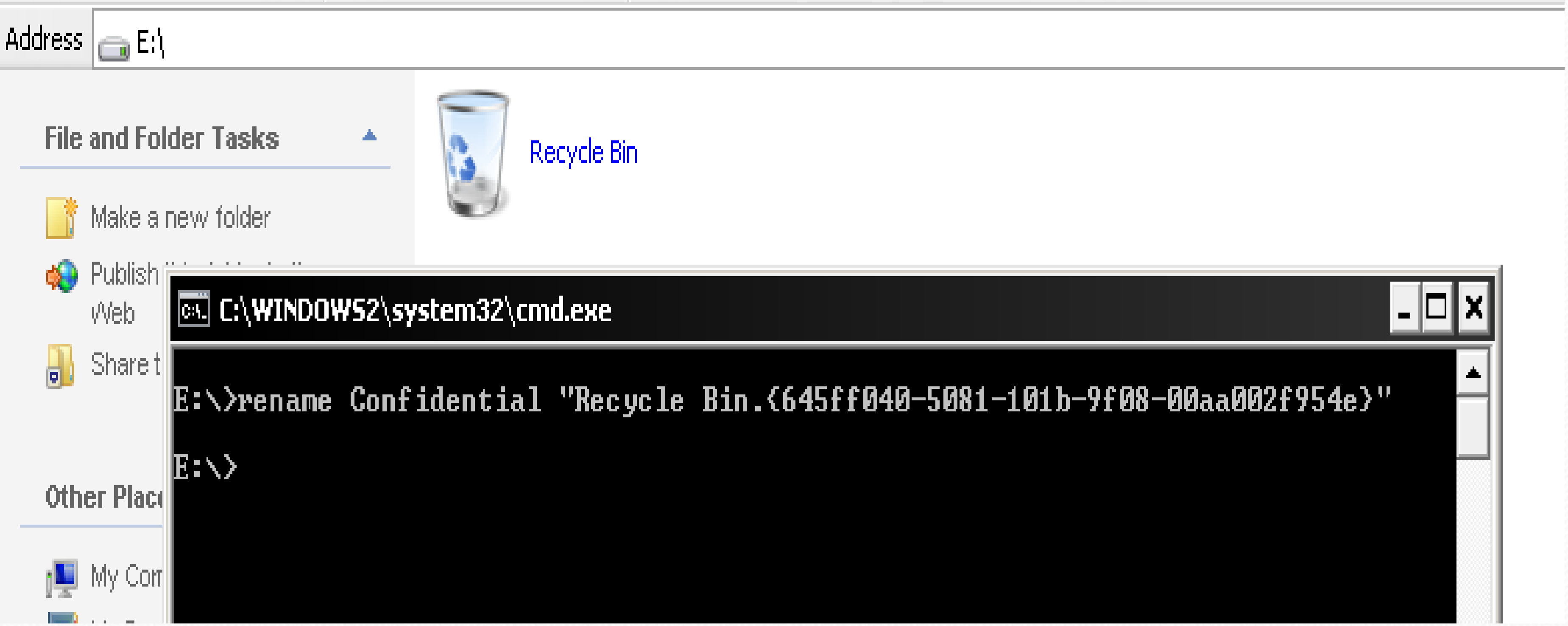
Source: http://www.autohotkey.com/docs/misc/CLSID-List.htm

Okay, So Why is CLSID included in this presentation ?

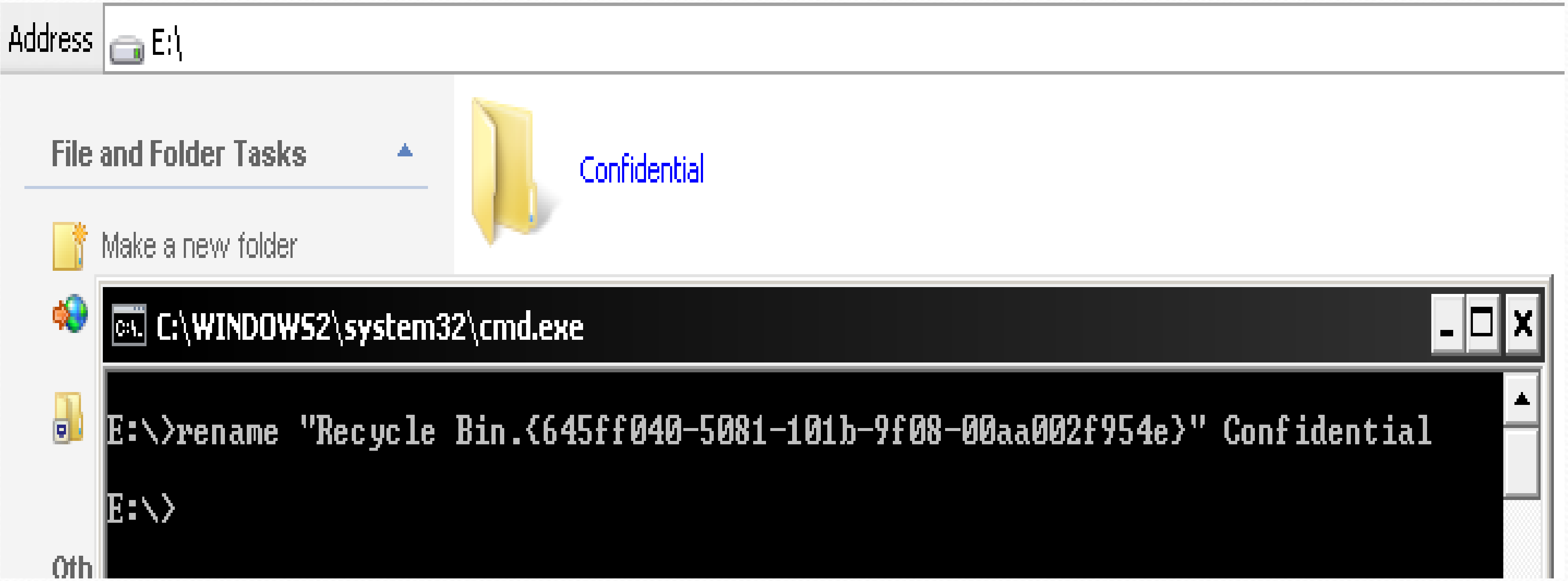
- The CLSID's can be assigned to any folder.
- If CLSID of any ***special*** folder is also assigned to ***any*** folder, the folder starts to act ***like*** the special folder.
- Therefore, the data inside the folder can be camouflaged.



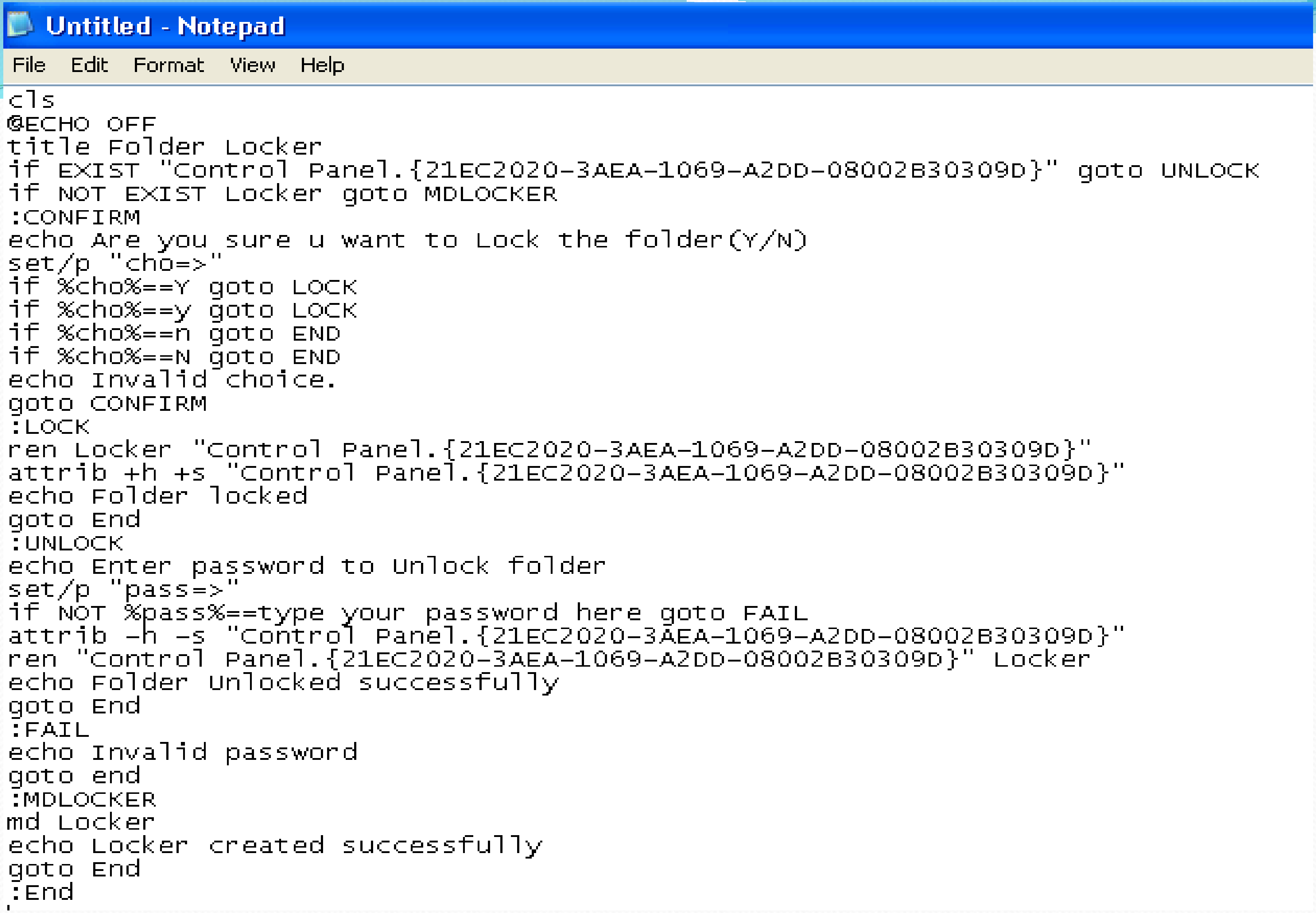
```
Company ABC, Inc. Trade Secrets :

On the Insert tab, the galleries include items that are
designed to coordinate with the overall look of your
document. You can use these galleries to insert tables,
headers, footers, lists, cover pages, and other document
building blocks. When you create pictures, charts, or
diagrams, they also coordinate with your current document
look. You can easily change the formatting of selected
text in the document text by choosing a look for the
selected text from the Quick Styles gallery on the Home
tab.
```



```
E:\>rename Confidential "Recycle Bin.{645ff040-5081-101b-9f08-00aa002f954e}"

E:\>
```



```
E:\>rename "Recycle Bin.{645ff040-5081-101b-9f08-00aa002f954e}" Confidential

E:\>
```



```
cls
@ECHO OFF
title Folder Locker
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Locker goto MDLOCKER
:CONFIRM
echo Are you sure u want to Lock the folder(Y/N)
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Locker "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Folder locked
goto End
:UNLOCK
echo Enter password to Unlock folder
set/p "pass=>"
if NOT %pass%==type your password here goto FAIL
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Locker
echo Folder Unlocked successfully
goto End
:FAIL
echo Invalid password
goto end
:MDLOCKER
md Locker
echo Locker created successfully
goto End
:End
```

NTFS

The File System of Microsoft XP

What is a File System ?

- A file system is a part of the operating system that determines how files are named, stored organized on a volume.
- A file system manages files and folders, and the information needed to locate and access these items by local and remote users.
- Microsoft Windows supports both the FAT and NTFS file systems.
- Linux supports ext2, ext3, Reiser FS, etc.
- Macintosh supports HFS.

What is NTFS ?

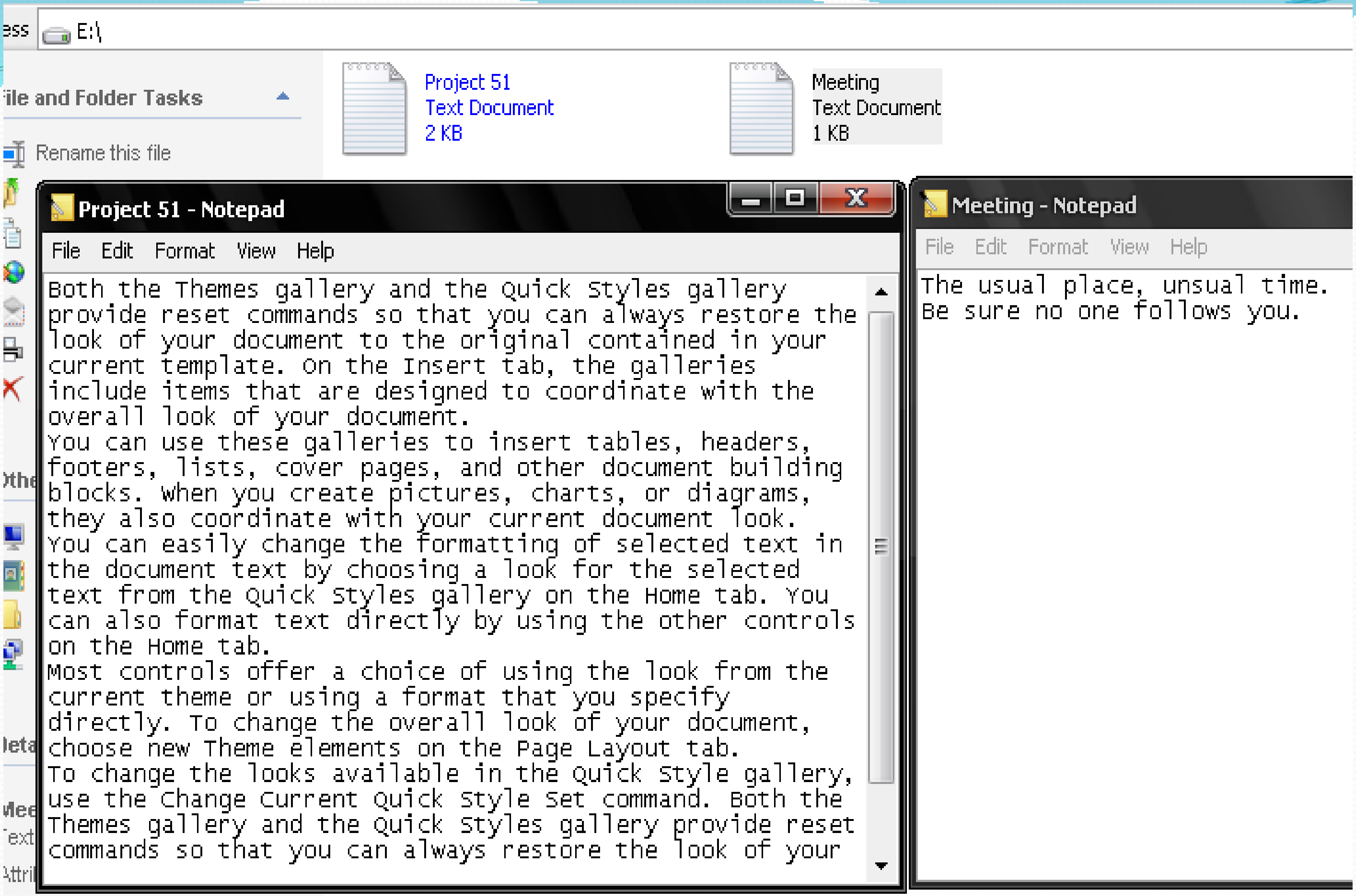
- It is the abbreviation of New Technology File System.
- It is the most secure and robust file system for Windows NT, 2000, and XP.
- What are the features of NTFS :
  - Supports compression,
  - Recoverable file system,
  - Supports Macintosh files,
  - Disk quotas,
  - Sparse files.

Alternate Data Stream (ADS)

- ADS was implemented in order to allow compatibility with the Hierarchical File System (HFS).
- HFS stores its data in two parts;
  - Resource fork.
  - Data fork.
- The Data fork is where the data is actually contained and the resource fork is used to tell the operating system how to use the data portion.
- Windows does the same thing through the use of extensions such as ***.bat*, *.exe*, *.txt*,** etc.

So what is wrong with ADS ?

- The First thing is they are totally hidden.
- A user can hide quite a lot of data in ADS and nobody will ever know it.
- Oh yes, and even a guest can create such streams in every file where he has write access for, how clever ?



Both the Themes gallery and the Quick Styles gallery provide reset commands so that you can always restore the look of your document to the original contained in your current template. On the Insert tab, the galleries include items that are designed to coordinate with the overall look of your document.

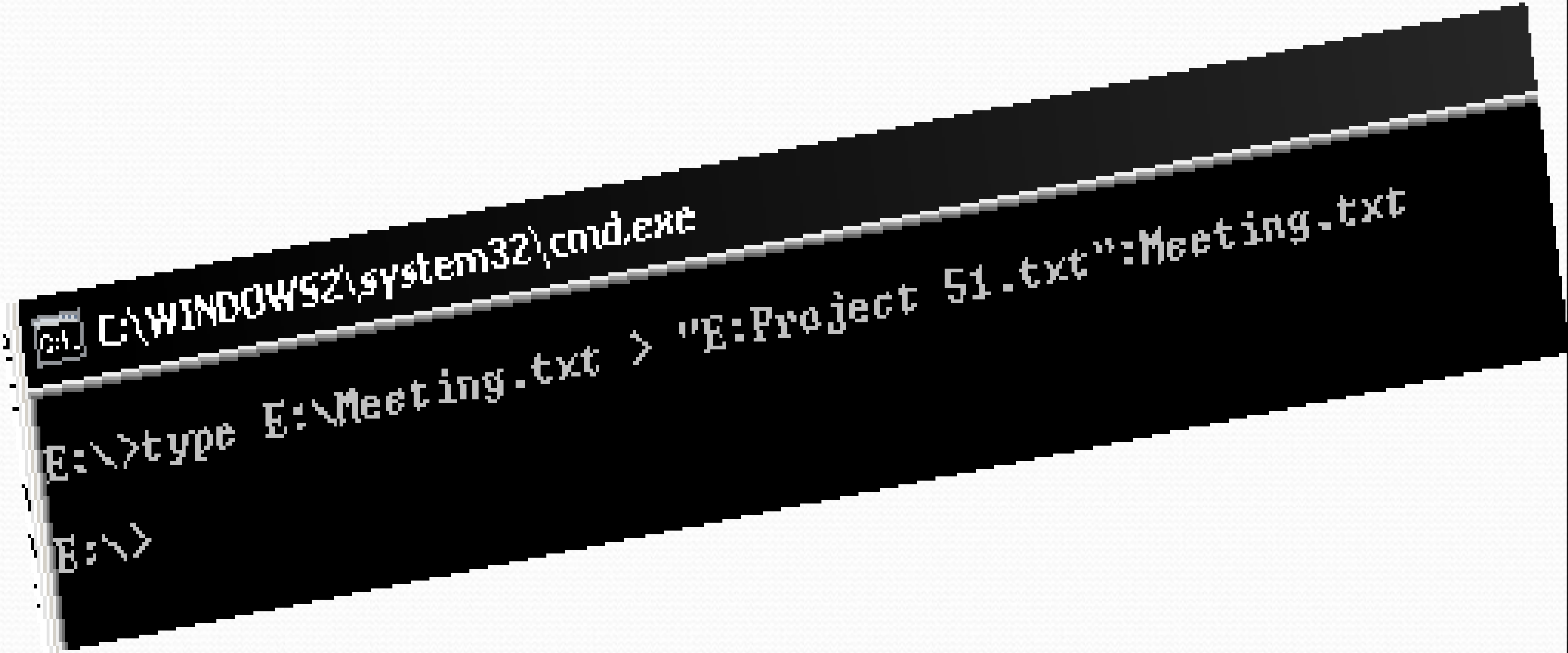
You can use these galleries to insert tables, headers, footers, lists, cover pages, and other document building blocks. When you create pictures, charts, or diagrams, they also coordinate with your current document look.

You can easily change the formatting of selected text in the document text by choosing a look for the selected text from the Quick Styles gallery on the Home tab. You can also format text directly by using the other controls on the Home tab.

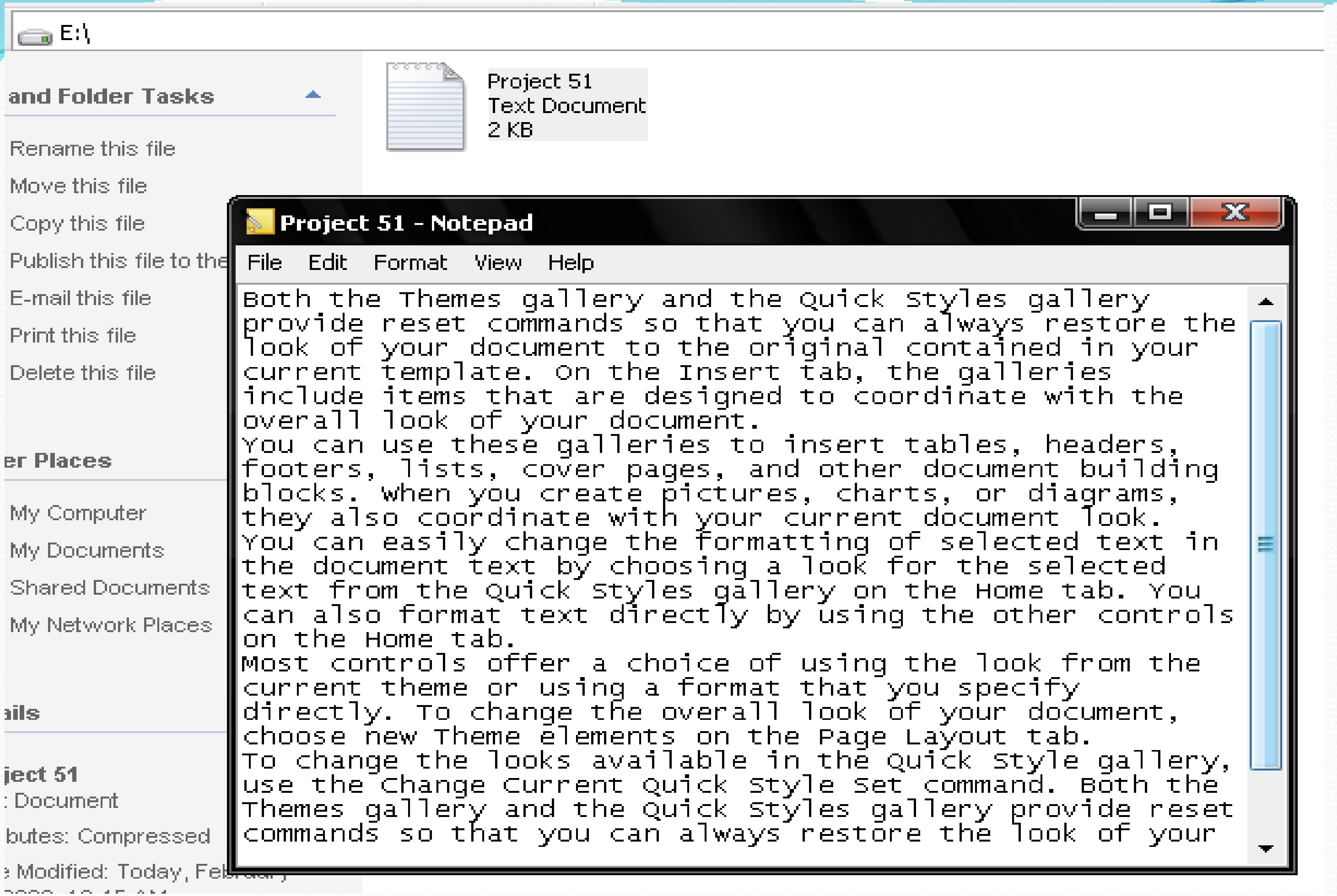
Most controls offer a choice of using the look from the current theme or using a format that you specify directly. To change the overall look of your document, choose new Theme elements on the Page Layout tab.

To change the looks available in the Quick Style gallery, use the Change Current Quick Style Set command. Both the Themes gallery and the Quick Styles gallery provide reset commands so that you can always restore the look of your

The usual place, unsual time.
Be sure no one follows you.



```
E:\>type E:\Meeting.txt > "E:Project 51.txt":Meeting.txt

E:\>
```



Both the Themes gallery and the Quick Styles gallery provide reset commands so that you can always restore the look of your document to the original contained in your current template. On the Insert tab, the galleries include items that are designed to coordinate with the overall look of your document.

You can use these galleries to insert tables, headers, footers, lists, cover pages, and other document building blocks. When you create pictures, charts, or diagrams, they also coordinate with your current document look.

You can easily change the formatting of selected text in the document text by choosing a look for the selected text from the Quick Styles gallery on the Home tab. You can also format text directly by using the other controls on the Home tab.

Most controls offer a choice of using the look from the current theme or using a format that you specify directly. To change the overall look of your document, choose new Theme elements on the Page Layout tab.

To change the looks available in the Quick Style gallery, use the Change Current Quick Style Set command. Both the Themes gallery and the Quick Styles gallery provide reset commands so that you can always restore the look of your

Another Big Problem …

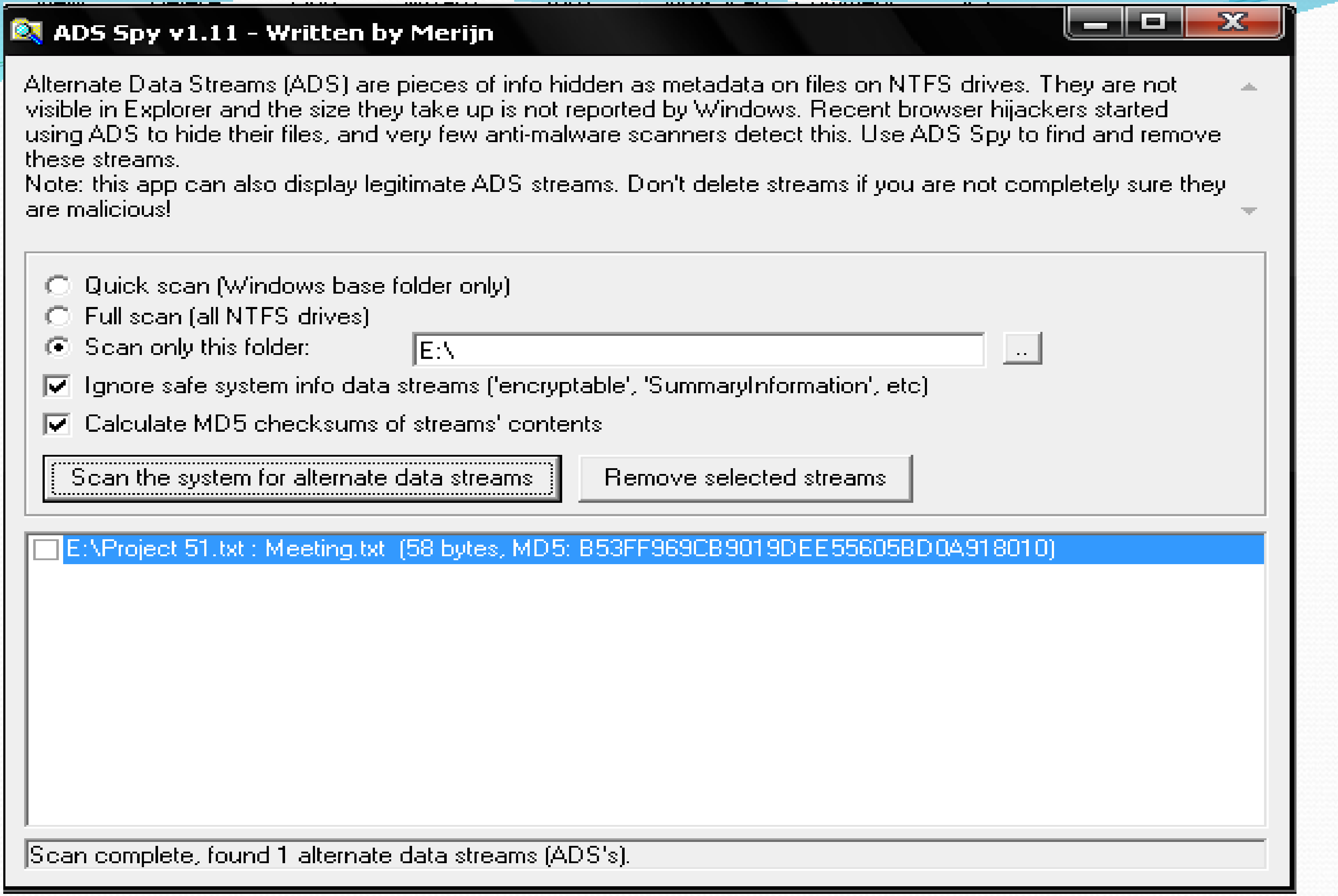
- Its not limited to text filers either ….
- Executables can also be hidden by the same manner, and on top of that, they can be executed even without extracting them back. Now I can Wow !
- I wonder why this is not being used by malware to hide themselves.
    - Download.fugif

Programs to find ADS

- ADS Spy - http://www.bleepingcomputer.com/files/adsspy.php

- LADS (List ADS) – http://www.heysoft.de/Frames/f_sw_la_en.htm

- Streams v1.56- http://www.microsoft.com/technet/sysinternals/FileA



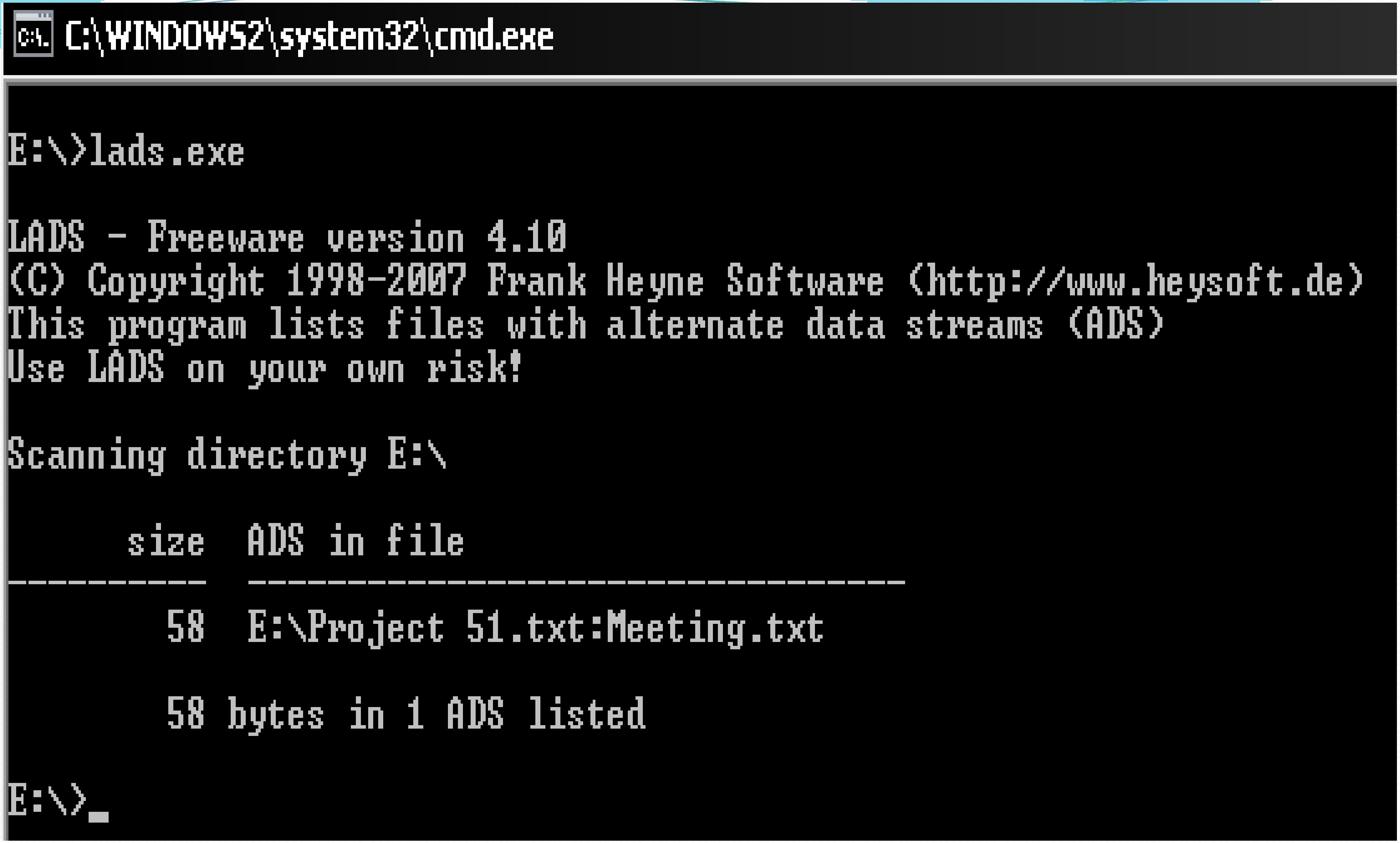
Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
○ Full scan (all NTFS drives)
● Scan only this folder: E:\

☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
☑ Calculate MD5 checksums of streams' contents

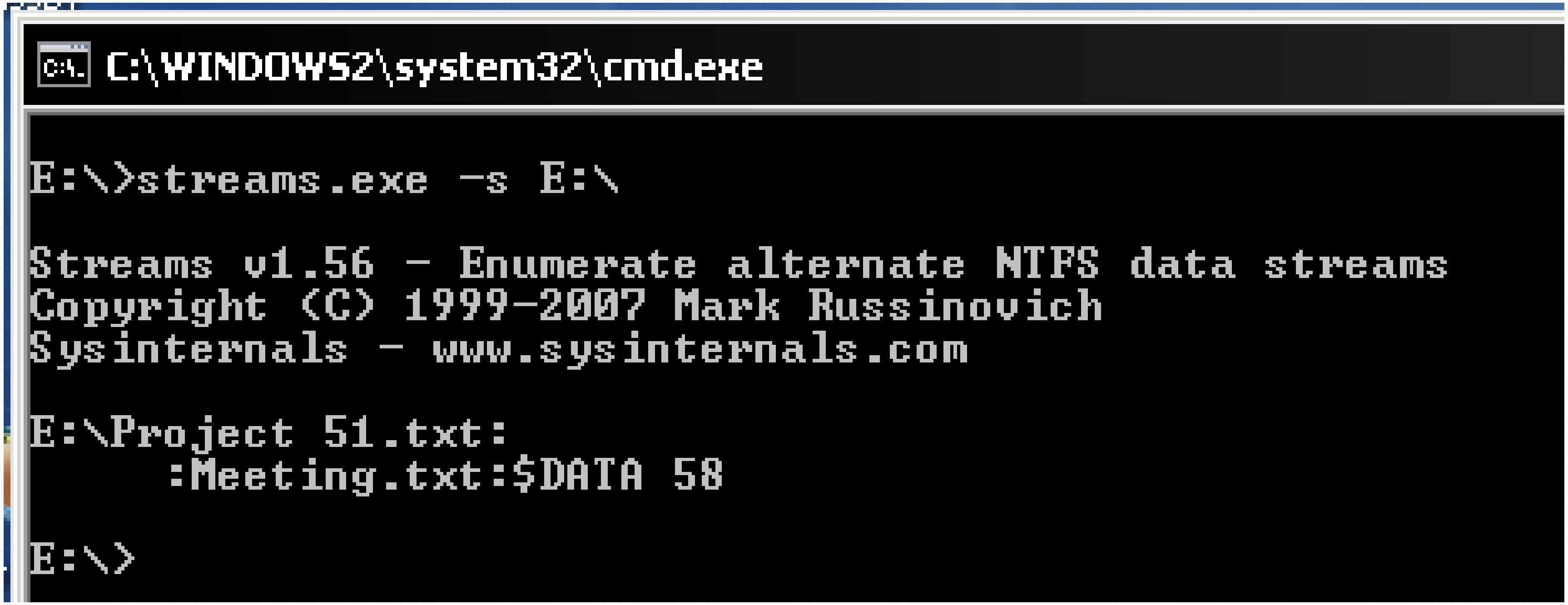
□ E:\Project 51.txt : Meeting.txt (58 bytes, MD5: B53FF969CB9019DEE55605BD0A918010)

Scan complete, found 1 alternate data streams (ADS's).



C:\WINDOWS2\system32\cmd.exe

```
E:\>lads.exe

LADS - Freeware version 4.10
(C) Copyright 1998-2007 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory E:\

      size  ADS in file
----------  ----------------------------------
        58  E:\Project 51.txt:Meeting.txt

        58 bytes in 1 ADS listed

E:\>_
```



```
E:\>streams.exe -s E:\

Streams v1.56 - Enumerate alternate NTFS data streams
Copyright (C) 1999-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

E:\Project 51.txt:
     :Meeting.txt:$DATA 58

E:\>
```

Questions ????

Prashant Mahajan
prashant3535@gmail.com
+91-9822426910

Thank You