

Objectives

1. To find information and uncover hidden files left by a suspect on their computer
2. To be the “perp” and hide secret information

Before you begin –

- Change the folder options so that you can “see” all file extensions and operating system files.
- Create a folder on the C drive to save your work C:\ Users\Student\yourname
- All the files are in a folder on the Desktop called **Dianes Utils**

1. Things are not always as they appear

Copy the files from **Exercises\Ex1.1** into your own folder on **C:\ Users\ Student\ yourname**

- a. Double click on the file **TestFile.htm** - Select **Open With** and **Internet Explorer**.

Q1. Does this file give any cause for concern? _____

- b. Right click on **TestFile.htm** - Select **Open With** and chose **MS Word** from the list.

- c. Using **Word** move down to the line that says **End of file**.

Q2. Is this the last line of the file? _____

Hint – hold the mouse down and drag to the bottom. Select Font colour and change this to black or automatic.

Now scroll to **Test of Wingdings2**. Highlight the Wingdings font and change this to Arial.

Q3 What do you see now? _____

Change the text back to Wingdings, save it and now open the file using FireFox – Is there a difference?

Q4. What is the best way to view this file? _____

- e. Open **TestFile.doc** and it appears to have the same content as TestFile.htm. Close the file. In **Explorer** right-click **TestFile.doc** and rename it by changing the file’s extension to **.xls** The file now appears to be an excel spreadsheet – double click it.

Q5. Would you expect this file it open correctly? _____

Q6. Does it actually open correctly? _____

- f. Double click on **test2.doc** – click **NO** if a message comes up about installing a feature to import the specified file format.

Q7. What type of file do you think this is?
Change the extension

Q8. Can you get it to open? _____

2. Capturing volatile information

Prior to switching off the power to a suspect machine, all volatile evidence should be captured.

Open up a **Command Prompt** window (see Appendix on how to do this)

On the C drive – type **DIR** to see the folders present

Change to the folder where the files are located – **cd C:\ Users\ Student\ Command-Line Tools**.
 Currently this has a space in it (which DOS does not like) press the **Tab** key or rename the folder.
 Check if you are in the correct folder by typing **DIR** to see the files present.
 Capture the information to a file using a pipe (>) command (see Appendix on how to do this)
 Type the following, once on its own and again to pipe it out to a text file called **save.txt**:-

date /t & time /t	<i>this shows you what the output will be for current date and time</i>
date /t & time /t > save.txt <enter>	<i>pipe (>) out to a file called save.txt</i>
netstat -nao	<i>-n displays addresses and port in numeric form</i>
	<i>-a displays all connections and listening ports</i>
	<i>-o displays the owning processsID associated</i>
netstat -naob	<i>add -b to display the executable involved</i>
netstat -nao >> save.txt	<i>processes running & the ports they have open</i>
netstat -r	<i>shows the routing table</i>
netstat -r >> save.txt	<i>pipe out to the file</i>
tasklist /v	<i>v for verbose – pipe out to the file >> save.txt</i>
tasklist /svc	<i>displays services in each process</i>
tasklist /svc >> save.txt	<i>service threads and the processes they are running under</i>
net user put- name-here >> save.txt	<i>user currently & historically logged on with date + times and</i>
	<i>append to save.txt (on these PCs user = Student)</i>

Also try Pslist, Psinfo, PSGetSID, Psfile, Psloglist and Psloggedon

Try the following on your own machine when connected to a network or in KW116

nbtstat	<i>current network connections – try the switches listed</i>
net sessions	<i>shows username, IP address and type used to access the system</i>
	<i>via remote login sessions</i>
net view /domain	<i>gives all the domains present</i>
net view /domain:a-name-from-list	<i>look at a specific domain</i>
net use	<i>NetBIOS Name Service on TCP 139</i>
net use \\192.168.202.33\IPC\$ "" /u:""	<i>/u: "" = built-in anonymous user with null password</i>

Q.9 What type of information did you gather? How useful would this be in your investigation?

In the command prompt window press <F7> key
 (If your keyboard has a function lock key <F Lock> ensure that the light is on.)

Q10. What information is displayed? _____
 { You could capture this information using the print screen function and save it to a file. }

3. Other Tools

Investigate the following tools. These need to be run on a command line.

- Open a Command Prompt from the main menu (Start).
- Change to the folder **cd C:\ Users\ Student\ Command-Line Tools**
- Check if you are in the correct folder by typing **DIR** –some of the files are listed below

Afind.exe	last access time finder (-? for help)
Audited	builds an audit list (-? for help)
DACLchk	dumps any ACL that has been Denied and Allowed ACEs in reverse order
FileStat.exe	dumps NTFS security, file and stream attributes
Hfind	hidden file finder with last access time (-? for help)

Hunt	SMB share enumerator and admin finder
Sfind	alternative data stream finder(-? for help)
PSGetSID	get the security ID from Windows

There are a number of other tools on the list that you can try as well
The output of all these could be piped out to a file using `>>filename.txt`

4. Perform Time Analysis on Your Files

In section 3 (Other Tools) you used Afind.exe. Copy this file to your folder.

Open a **Command Prompt** and use **Afind** to determine when the files that you have just been using were last accessed. Pipe the results out to a file.

Q11. Can you see the order in which they were accessed? _____

5. Creating Alternate Data Streams

Note—the default folder is C:\Users\Student\

- i. Type **notepad test.txt** and click **yes** to create the file on the C drive
- ii. Type some text into the file and save the file – note where you saved the file.
- iii. Close the file. [Do not close the Command Prompt window]
- iv. Type **Dir** to list the files and note the size of your file and the free space available.

File size _____ Bytes Free _____

- v. Type the following in the command prompt to create an ADS

```
echo secret password > test.txt:hidden.txt
```

- vi. Check the file sizes again – Did the file size change?

Test.txt_____bytes Bytes free_____bytes

- vii. Try using a large number of characters – more than shown here.

[illegible]

- viii. Check the file sizes again – you should see a difference in free space now

Test.txt_____ bytes Bytes free_____ bytes

Using Streams to identify ADSs

In the **Command Prompt** window locate the folder called Commandline Tools (see above) and navigate to it by typing **dir** and then **cd streams**

Type **Streams** /? *To see Help*

Type **streams -s c:\User\Student** *full path name to your folder*

Q12. Did the Streams tool locate your test.txt file? _____

Q13. How many ADS's does it have? _____

Using LADs to locate an ADSs

In the Command Prompt change to the folder

cd Command-Line Tools\lads <enter> *changes directory to lads*

LADs /A c:\User\Student *should locate your file – test.txt – also try /s*

Q14. Did the LADS tool locate your test.txt file? _____

Advanced (don't worry if you can't do this part)

Try to embed an executable in an ADS – use the file notepad.exe

Create a text file called test2.txt. Copy an executable into your working folder (there are some in the Exercises folder)

Type *filename.exe*>test2.txt:*filename.exe* - where *filename* is the executable

Check your file for an ADS using both Streams and LADs

Q15. What can you see now? _____

- i. Use **notepad** to verify that your file contents is still the same. Use DIR again and check if anything has changed.

Q16. What has changed? _____

You have embedded an executable into a text file, which can be launched.

Open the **Task Manager** and ensure that **note.exe** is not currently running.

Leave the Task manager running.

From the Command Prompt type in: **start .\test2.txt:note.exe**

Q17. What happened? Can you see note.exe in the Task manager? _____

6. Type msinfo32 in the MS Start Menu

In System Information select **Software Environment** and **Running Tasks**

Select **File | Export** and in the Export As window specify a filename – sysinfo1 – and save

Under **Software Environment** click **Startup Programs**

Select **File | Export** and in the Export As window specify a filename – use **sysinfo2** – and save

7. Using your save.txt and the sysinfo files answer the following:-

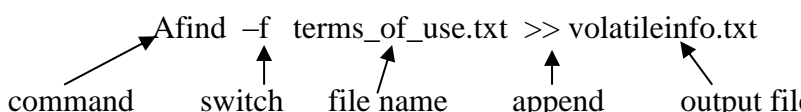
Q18. How long has this system been up and running?

Q19. Has anyone else been logged on to this machine?

Appendix

Open a Command Prompt – either select it from the **Programs menu | Accessories | Command Prompt** or use **Start | Run** and type **cmd**

Pipe the output to a file – run the command and display it to the screen (default) to check the information. Then capture the information by piping it to a file instead of to the screen.

 *{ appends output to a file called volatileinfo.txt }*