**DIGITAL FORENSICS LAB**

|  |  |
| --- | --- |
| Exercise 6 | |
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulagara |
| Date | 21st September, 2021 |

**AIM**

To write about some file extensions.

**EXTENSIONS**

A few extensions are listed out and described below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EXTENSION | FILE TYPE | OPENS WITH | CROSS-PLATFORM | DESCRIPTION |
| JPG/JPEG | Image | Any photo viewer (like Photos) | Yes | * It uses lossy compression * Used for images commonly and digital photography * Other extensions .jpe, .jif, .jfif * Degree of compression can be adjusted |
| PNG | Image | Any photo viewer | Yes | * Stands for Portable Network Graphics * It supports lossless compression * Designed for images to be transferred over the internet * Non-RGB colour spaces not supported * Contains encoded pixels in a series of “chunks” |
| GIF | Image | Any photo viewer | Yes | * Stands for Graphics Interchange Format * Supports up to 8 bits per pixel * Compressed using the lossless data compression technique LZW * Can contain up to 255 colours |
| TIF / TIFF | Image | Any photo viewer | Yes | * Stands for Tag Image File Format * Uses lossless (LZW) or no compression * Can be used as a container for JPEG and PNG files |
| BMP | Image | Any photo viewer and graphics application | Yes | * Stands for Bitmap file * Has a file header size of 14 bytes * Older GUIs use bitmaps in their built-in graphics subsystem * Large file size due to low ratio or no compression |
| ART | Image | Image Viewer apps | Yes | * Highly compresses an image * Designed to facilitate quick download |
| PCX | Image | Image viewer apps | Yes | * Stands for Picture Exchange * Not used a lot anymore * Uses little endian byte ordering |
| WMF |  |  |  |  |
| EMF |  |  |  |  |
| DWG |  |  |  |  |
| PSD |  |  |  |  |

**JPG and JPEG**

**Type of file**

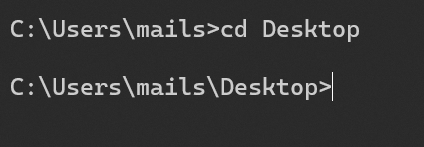
Images

**DESCRIPTION**

Commonly used method of lossy compression of digital images. Typically used with

**cd**

**OUTPUT**

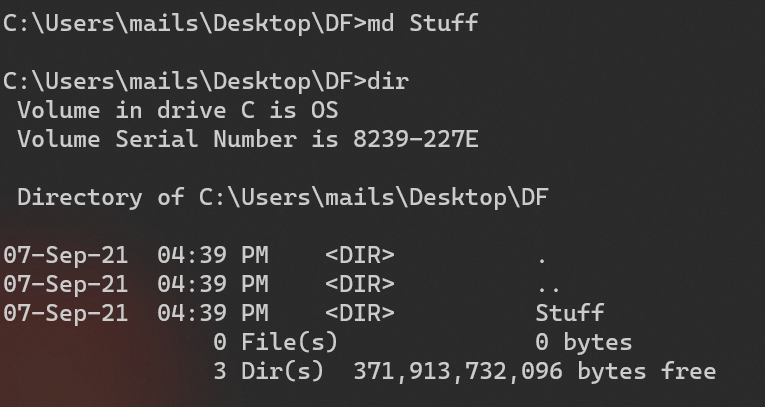


**DESCRIPTION**

Used to change the working directory.

**md**

**OUTPUT**

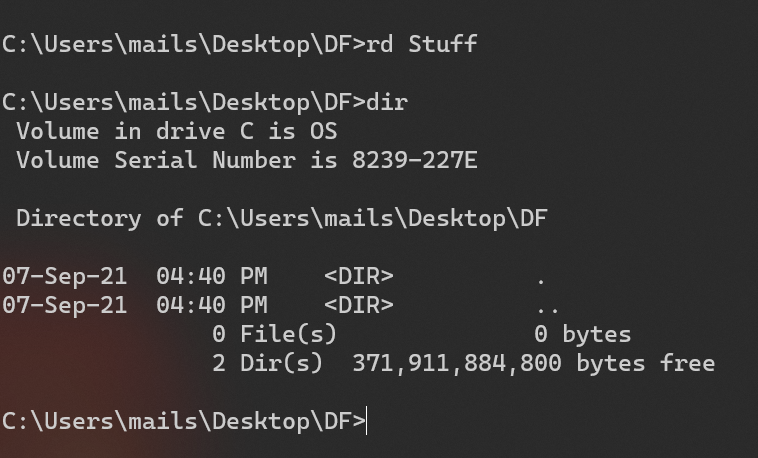


**DESCRIPTION**

Used to make a new empty directory.

**rd**

**OUTPUT**

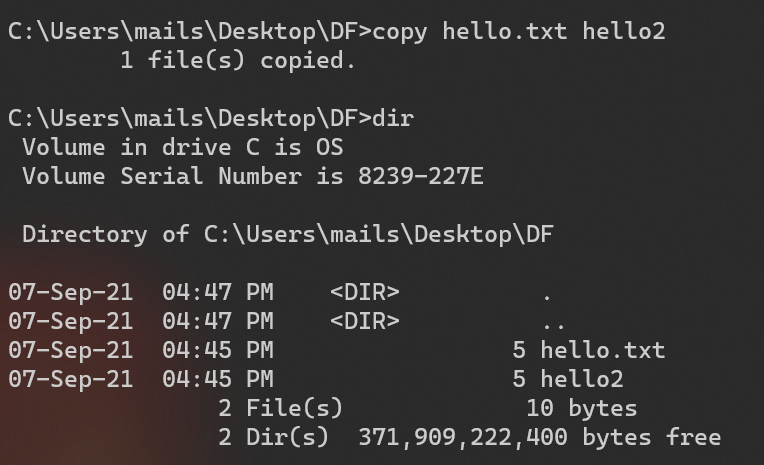


**DESCRIPTION**

Used to make remove a directory and its contents.

**copy**

**OUTPUT**

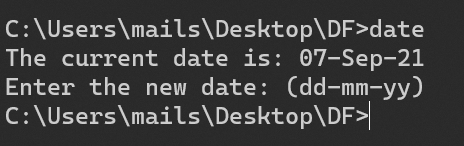


**DESCRIPTION**

Used to copy files. In the above picture, hello.txt was copied and saved as hello2 in the same directory.

**date**

**OUTPUT**

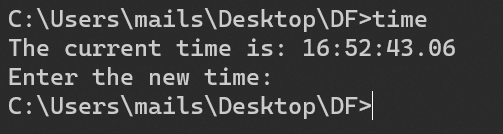


**DESCRIPTION**

Used to display and reset date.

**time**

**OUTPUT**

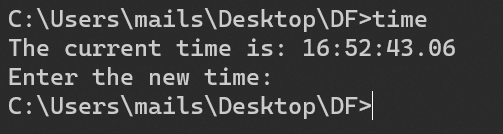


**DESCRIPTION**

Used to display and reset time.

**vol**

**OUTPUT**

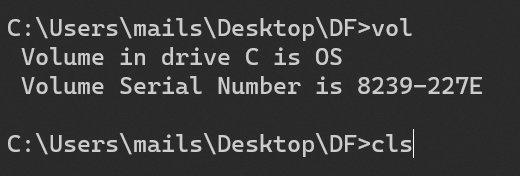


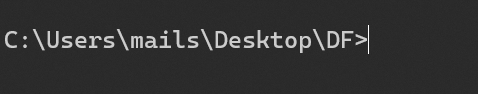
**DESCRIPTION**

Used to display the volume label and volume serial number of a logical drive.

**cls**

**OUTPUT**



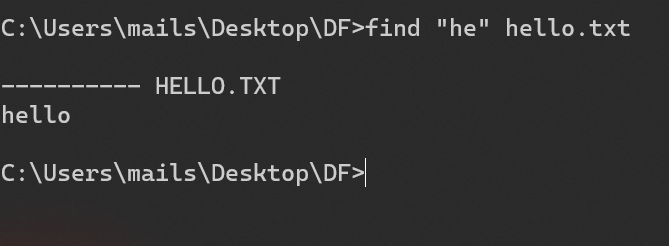


**DESCRIPTION**

Used to clear the console.

**find**

**OUTPUT**



**DESCRIPTION**

Used search for a string of text in a file or multiple files.

**EXERCISE**

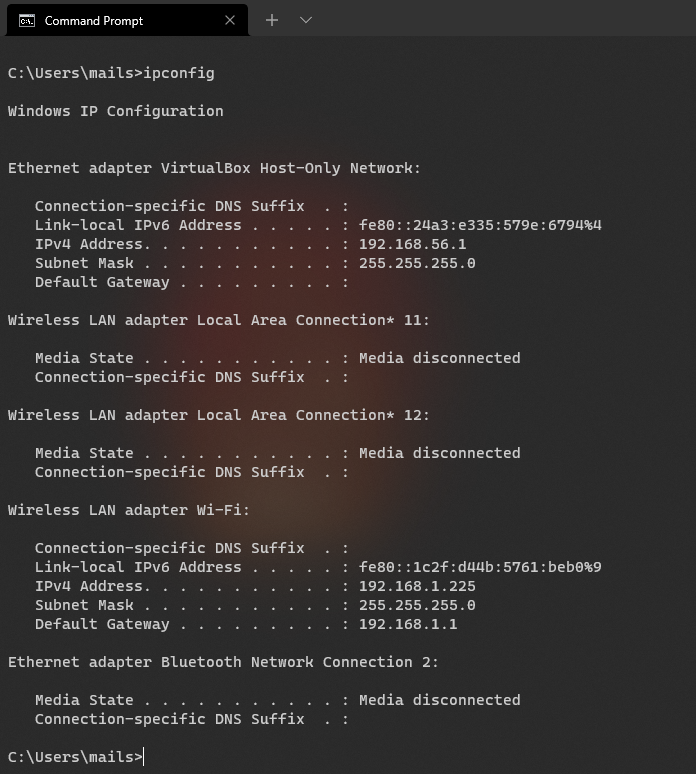
**TASK 1**

Use commands to find the IPv4 address and subnet mask of your computer

**COMMAND**

ipconfig

**OUTPUT**



**OBSERVATION**

This gives all IP information for all the network adapters in use by Windows. We see two adapters listed. The first one ‘Ethernet adapter VirtualBox Host-Only Network’ tells us that this system uses a hypervisor to manage virtual machines that have access to the internet. It has an IPv4 address of 192.168.56.1 and a subnet mask 255.255.255.0. The second, ‘Wireless LAN adapter Wi-Fi’ has an IPv4 address of 192.168.1.255 and the same subnet mask, 255.255.255.0.

**TASK 2**

Create a batch file that will capture the following volatile information from an evidence system and store it a file.

* Current IPv4 address
* Current date
* Current time
* ARP table
* Network connection information

**STEPS AND COMMANDS**

1. Open a text editor and type in the following:

@ECHO OFF

echo "IPv4 Adresses"

ipconfig | findstr /R /C:"IPv4 Address" /C:"Subnet Mask"

echo.

echo "Date is "

date /t

echo.

echo "Time is"

time /t

echo.

echo "ARP table is"

arp -a

echo.

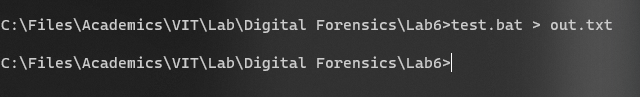
echo "Network Connection information"

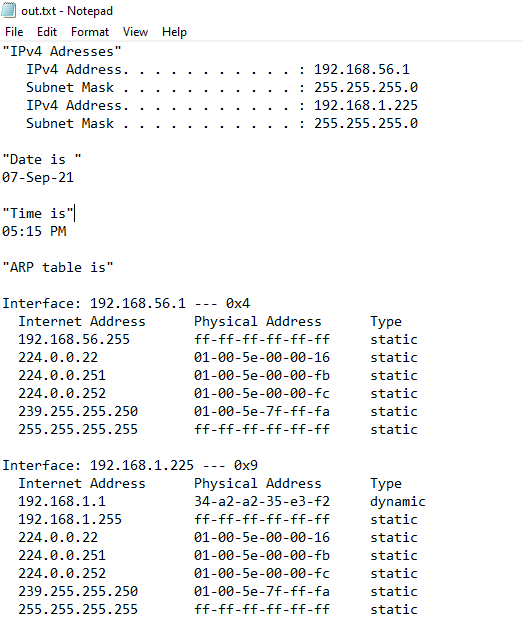
ipconfig

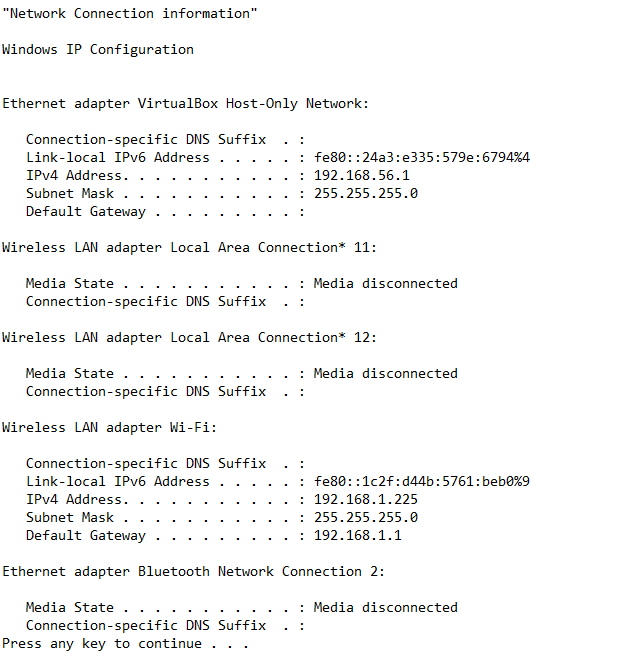
PAUSE

1. Then save it with an extension of “.bat” and select “ANSI” as encoding. Let the type remain as Text Document.
2. Then, double click on the newly created BAT file and verify output.

**OUTPUT**







**OBSERVATION**

Batch files can be used to run a collection of commands and see all their output at once, which makes it easier to work with rather than executing these commands one at a time. The output was then saved into a text file called “out.txt”.

**CONCLUSION**

We have worked with the Windows CLI and with Batch files to retrieve useful information about the device at hand and the network it is connected to.