DIGITAL FORENSICS LAB

Exercise 5	
Name	S Shyam Sundaram
Registration Number	19BCE1560
Slot	L39+L40
Faculty	Dr. Seshu Babu Pulagara
Date	7th September, 2021

AIM

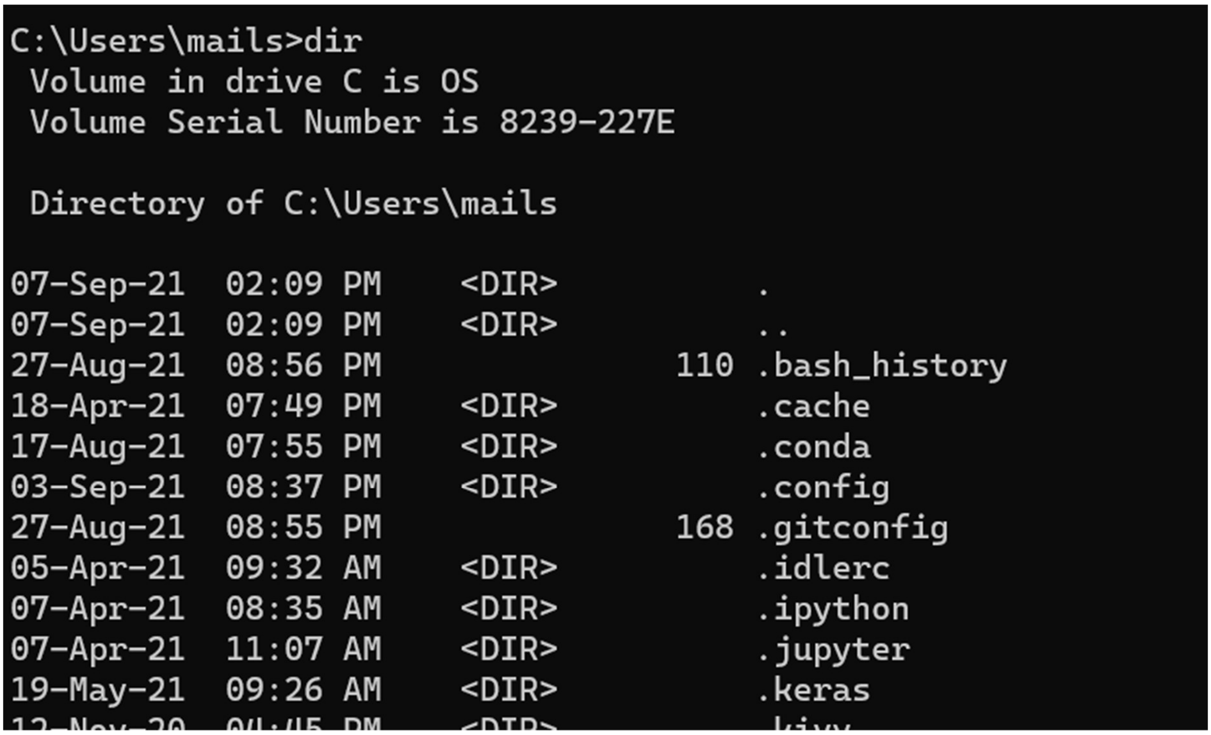
To work with the Windows Command Line.

SOME COMMANDS

A few commands are executed and their outputs are shown below.

dir

OUTPUT



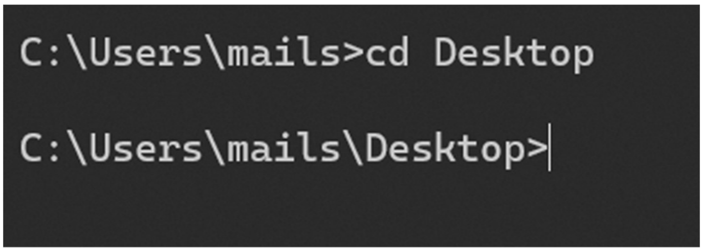
```
C:\Users\mails>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Users\mails

07-Sep-21  02:09 PM    <DIR>          .
07-Sep-21  02:09 PM    <DIR>          ..
27-Aug-21  08:56 PM               110 .bash_history
18-Apr-21  07:49 PM    <DIR>          .cache
17-Aug-21  07:55 PM    <DIR>          .conda
03-Sep-21  08:37 PM    <DIR>          .config
27-Aug-21  08:55 PM               168 .gitconfig
05-Apr-21  09:32 AM    <DIR>          .idlerc
07-Apr-21  08:35 AM    <DIR>          .ipython
07-Apr-21  11:07 AM    <DIR>          .jupyter
19-May-21  09:26 AM    <DIR>          .keras
12-Nov-20  04:45 PM    <DIR>          .kivy
```

DESCRIPTION

Displays information about files, directories and disk space occupied.

cd

OUTPUT



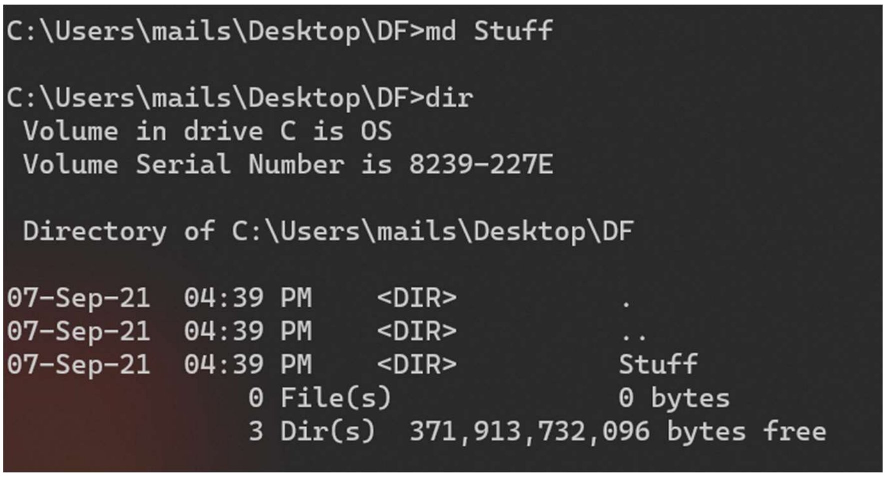
```
C:\Users\mails>cd Desktop

C:\Users\mails\Desktop>
```

DESCRIPTION

Used to change the working directory.

md

OUTPUT



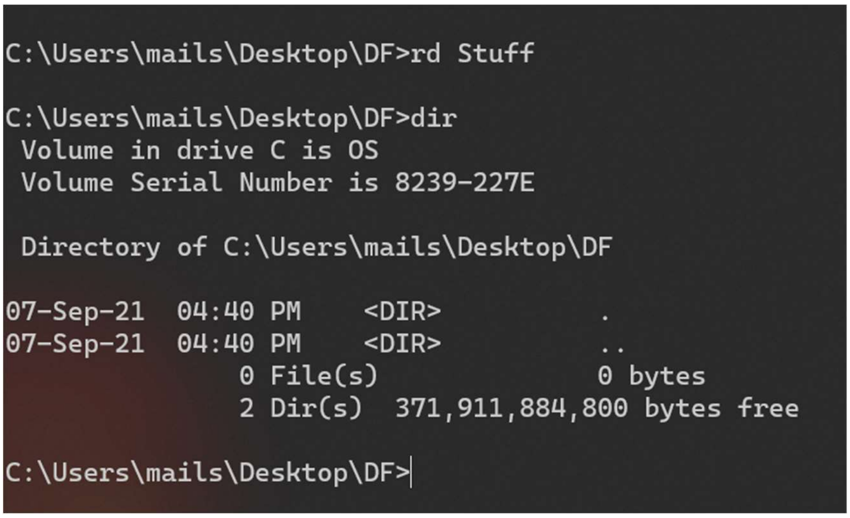
```
C:\Users\mails\Desktop\DF>md Stuff

C:\Users\mails\Desktop\DF>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Users\mails\Desktop\DF

07-Sep-21  04:39 PM    <DIR>          .
07-Sep-21  04:39 PM    <DIR>          ..
07-Sep-21  04:39 PM    <DIR>          Stuff
               0 File(s)              0 bytes
               3 Dir(s)  371,913,732,096 bytes free
```

DESCRIPTION

Used to make a new empty directory.

rd

OUTPUT



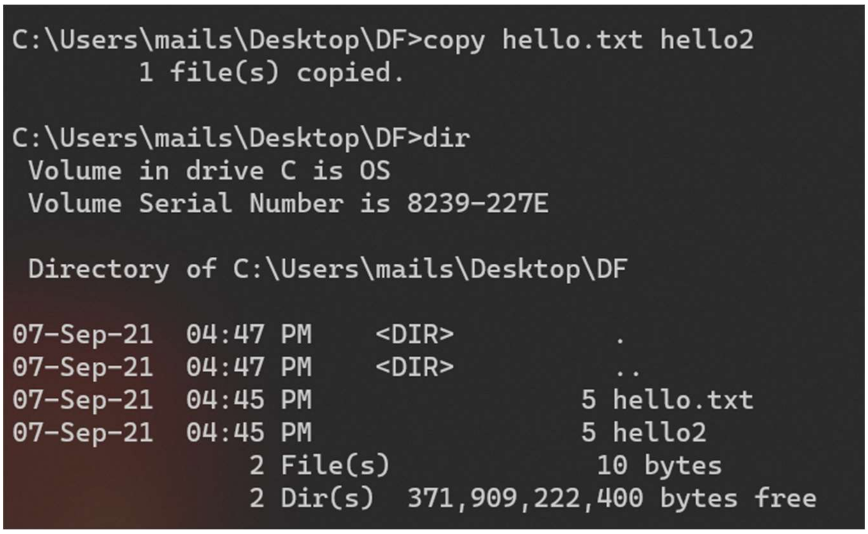
```
C:\Users\mails\Desktop\DF>rd Stuff

C:\Users\mails\Desktop\DF>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Users\mails\Desktop\DF

07-Sep-21  04:40 PM    <DIR>          .
07-Sep-21  04:40 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  371,911,884,800 bytes free

C:\Users\mails\Desktop\DF>
```

DESCRIPTION

Used to make remove a directory and its contents.

copy

OUTPUT



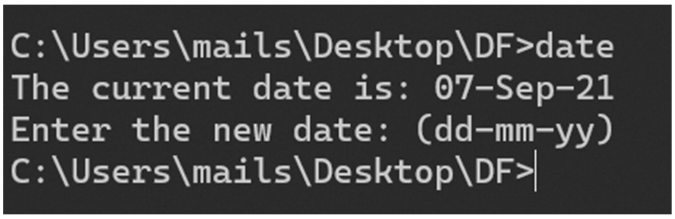
```
C:\Users\mails\Desktop\DF>copy hello.txt hello2
        1 file(s) copied.

C:\Users\mails\Desktop\DF>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 Directory of C:\Users\mails\Desktop\DF

07-Sep-21  04:47 PM    <DIR>          .
07-Sep-21  04:47 PM    <DIR>          ..
07-Sep-21  04:45 PM                 5 hello.txt
07-Sep-21  04:45 PM                 5 hello2
               2 File(s)             10 bytes
               2 Dir(s)  371,909,222,400 bytes free
```

DESCRIPTION

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

date

OUTPUT



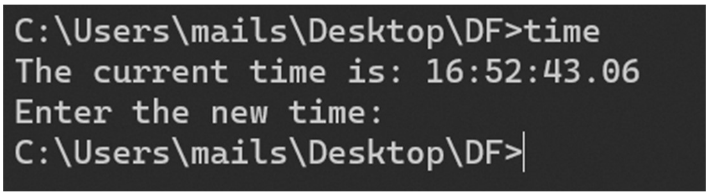
```
C:\Users\mails\Desktop\DF>date
The current date is: 07-Sep-21
Enter the new date: (dd-mm-yy)
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

Used to display and reset date.

time

OUTPUT



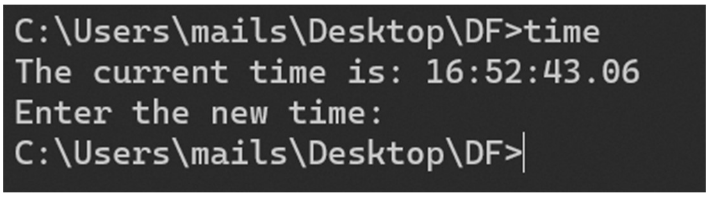
```
C:\Users\mails\Desktop\DF>time
The current time is: 16:52:43.06
Enter the new time:
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

Used to display and reset time.

vol

OUTPUT



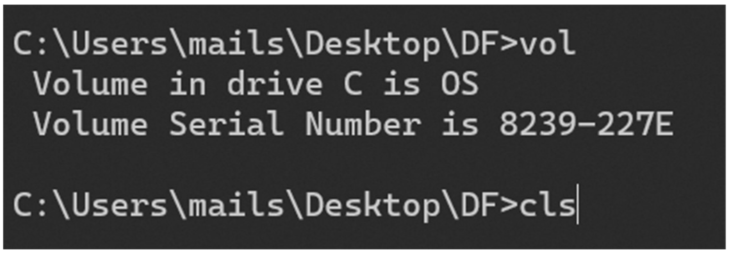
```
C:\Users\mails\Desktop\DF>time
The current time is: 16:52:43.06
Enter the new time:
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

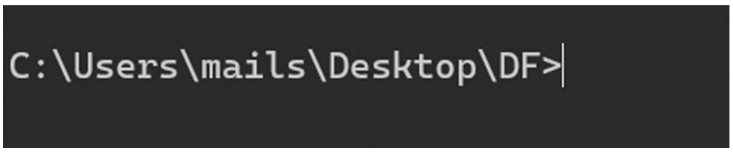
Used to display the volume label and volume serial number of a logical drive.

cls

OUTPUT



```
C:\Users\mails\Desktop\DF>vol
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

C:\Users\mails\Desktop\DF>cls
```



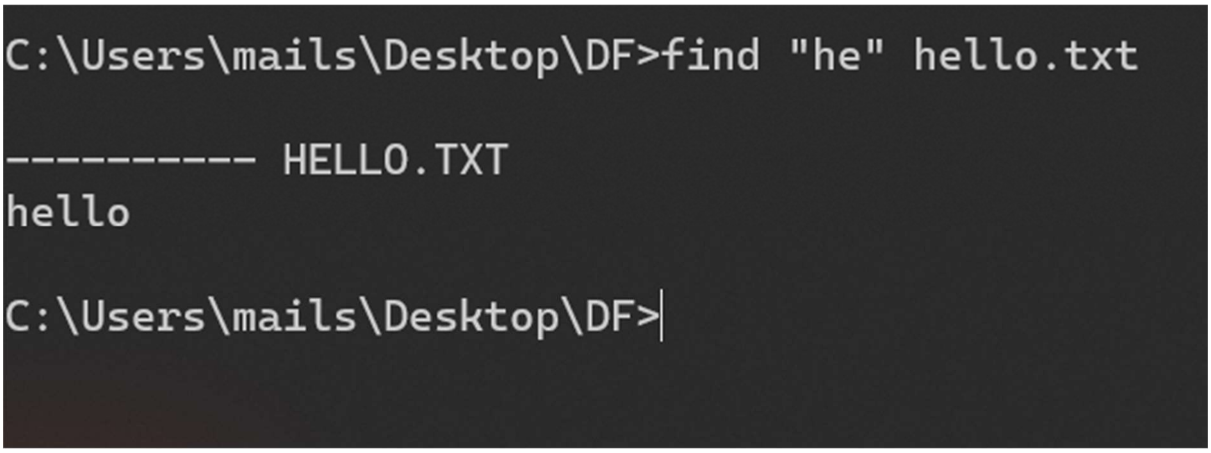
```
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

Used to clear the console.

find

OUTPUT



```
C:\Users\mails\Desktop\DF>find "he" hello.txt

---------- HELLO.TXT
hello

C:\Users\mails\Desktop\DF>
```

DESCRIPTION

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

EXERCISE

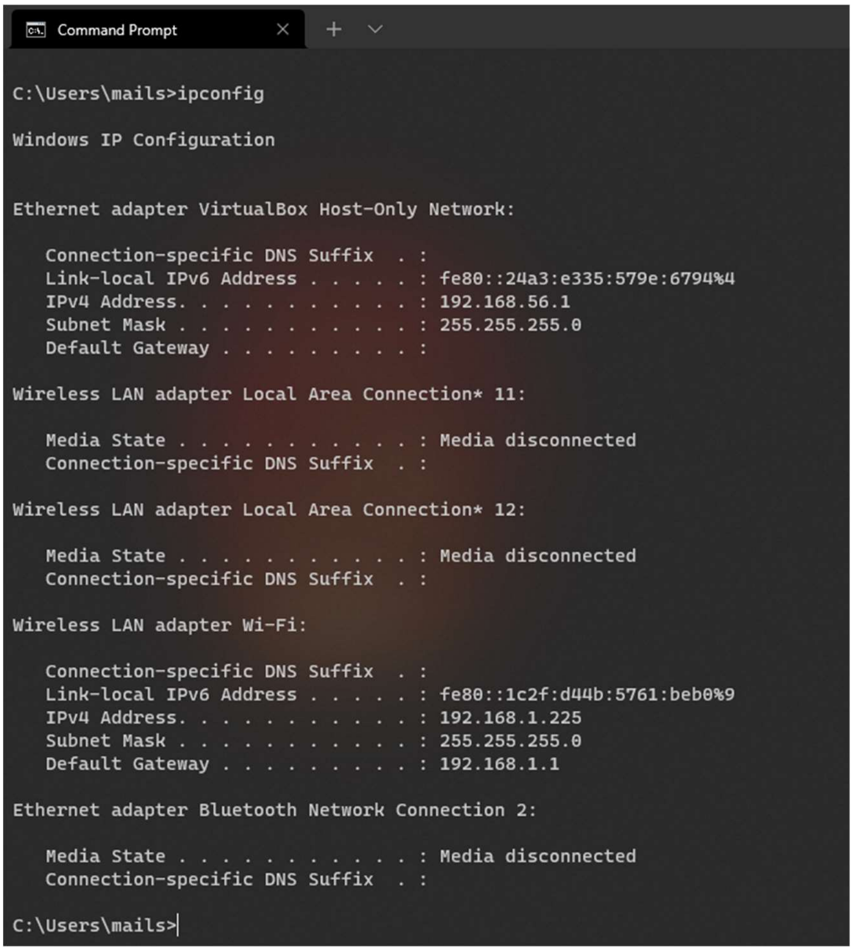
TASK 1

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

COMMAND

ipconfig

OUTPUT



```
C:\Users\mails>ipconfig

Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::24a3:e335:579e:6794%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c2f:d44b:5761:beb0%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.225
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\mails>
```

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

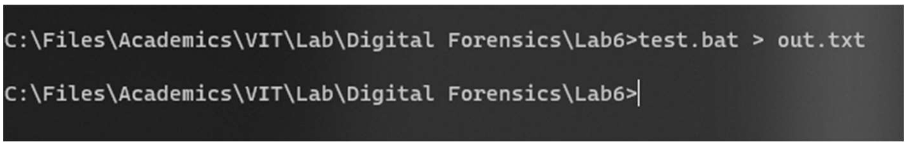
Create a batch file that will capture the following volatile information from an evidence system and store it a file.

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

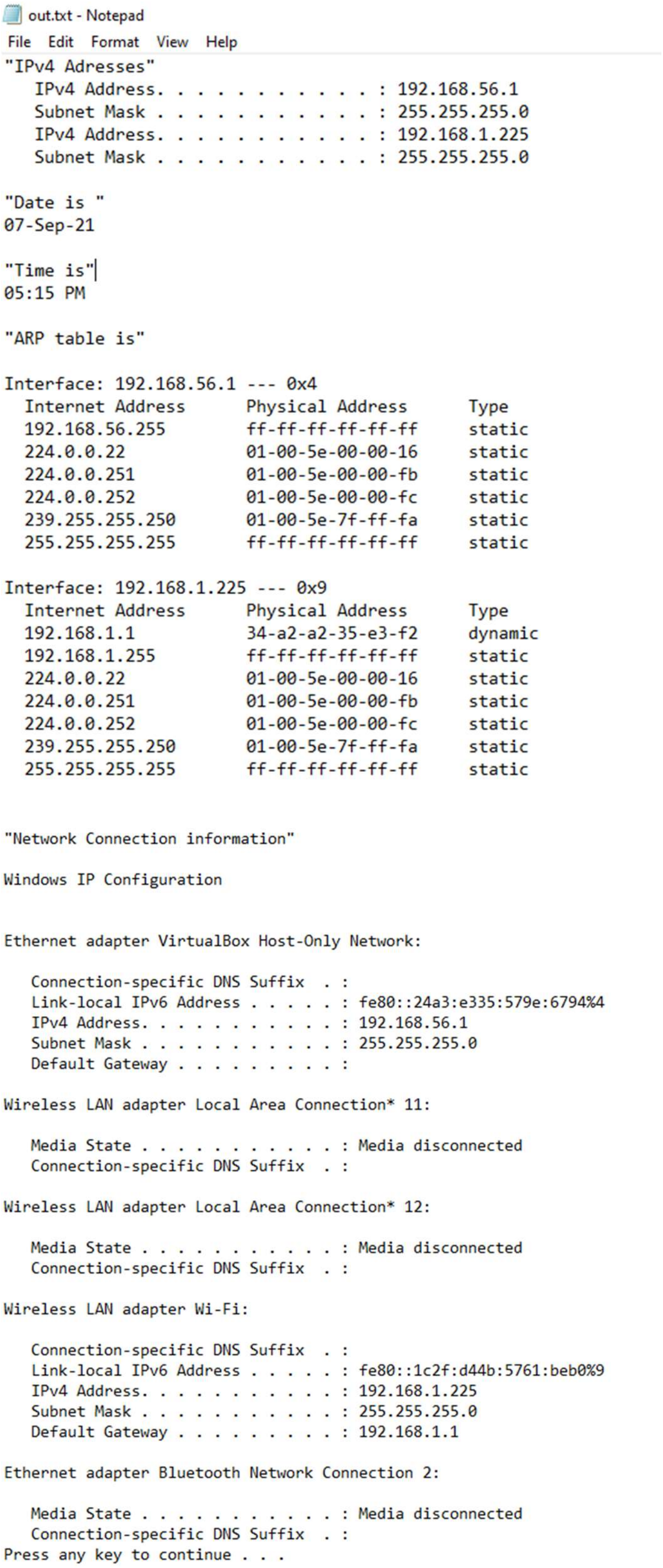
STEPS AND COMMANDS

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

OUTPUT



```
C:\Files\Academics\VIT\Lab\Digital Forensics\Lab6>test.bat > out.txt

C:\Files\Academics\VIT\Lab\Digital Forensics\Lab6>
```



```
"IPv4 Adresses"
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 192.168.1.225
   Subnet Mask . . . . . . . . . . . : 255.255.255.0

"Date is "
07-Sep-21

"Time is"
05:15 PM

"ARP table is"

Interface: 192.168.56.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.1.225 --- 0x9
  Internet Address      Physical Address      Type
  192.168.1.1           34-a2-a2-35-e3-f2     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static


"Network Connection information"

Windows IP Configuration


Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::24a3:e335:579e:6794%4
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c2f:d44b:5761:beb0%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.225
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Press any key to continue . . .
```

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.

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	Image	Image viewer apps	Yes	• Originally not device independent • Now is cross platform • Acts similar to SVG files • EMF+ is an extension to these • Consists of a series of records played to produce graphical content
DWG	Binary	Any CAD programs like AutoCAD	Yes	• Used to store two- and three-dimensional design data and meta data • It’s licensed by AutoCAD and is trademarked

PSD	Image	Photoshop, Illustrator, CorelDRAW	Yes	• Stands for photoshop document • Can hold layers with masks, alpha channels, text etc
RTF	Text	Word processors	Yes	• Stands for Rich Text Format • Standard RTF consists of only 7-bit ASCII characters with escape sequences
XML	Document (plain text)	Browsers	Yes	• Stands for eXtensible Markup Language • Uses tags to describe components in a file
HTML/HTM	Document (plain text)	Browser	Yes	• Hyper Text Markup Language • Used with CSS, JavaScript and other web content files
PHP3, PHP4, PHTML	Plain-text file for code	Code or text editors (VS Code)	Yes	• Used to develop web applications • Processed by a PHP engine on web browser • Can also be executed with command line
SHTML	Document (plain text)	Code or text editors	Yes	• It's an HTML file that includes server instructions • Similar to ASP file
EML	Email	Mail programs like Outlook	Yes	• Standard for Outlook Express • Used to store email files • Stores each message as a file
DBX	Email	Outlook	Yes	• Contains messages for a mailbox • Created by Outlook Express
PST	Message and mail	Microsoft Outlook, Exchange Client and Messaging	Yes	• Personal Storage Table • Used to store copies of messages, calendar events etc.

XLS	Spreadsheet	Microsoft Excel and other spreadsheet programs	Yes	• Native to Microsoft Excel • Can be opened by almost any spreadsheet program using APIs • Newer versions use xlsx
DOC/DOCX/DOT	Word document	Word processors	Yes	• Native to MS Word • But can be opened with other processors like Google Docs, Libre etc • Docx uses open XML format • Doc is older • Docx is smaller and easier to store • DOT extension files are templates created by MS Word to have preformatted settings for generation of doc and docx files
PPT/PPS	Slideshow	MS PowerPoint and any other slide show program	Yes	• PPT are PowerPoint files • PPT files are used to design slide shows • PPS files open in Slide Show mode when opened
PDF	Document	Any PDF viewer like Reader, Okular	Yes	• Portable Document Format • Developed by Adobe • Encapsulates a description of flat document • Contains 7-bit ASCII characters • Format is a subset of Carousel Object Structure (COS)
ZIP	Archive	Any compression program	Yes	• Can contain directories • Losless data compression

				• DEFLATE is the most commonly used algorithm • Minimum size of a zip file is 22 bytes •
RAR	Archive	WinRAR	Yes	• Proprietary format • Supports error correction • Creates smaller files than ZIP
GZ	Archives	Any compression tool like PeaZip	Yes	• Created by GNU zip compression algorithm • Uses DEFLATE, a combination of LZ77 and Huffman coding
BZ2	Archive	Compression tools like WinZip	Yes	• Made with open source BZIP2 compression method • Produces smaller files
ARJ	Archive	Tools like 7-Zip, WinRAR	Yes	• Stands for Archived by Robert Jung • Creates high-efficiency compressed files • Used to store backup of multiple files
WAV	Audio	Audio player	Yes	• Developed by IBM and Microsoft • Used for uncompressed as well as compressed audio
AVI	Audio/Video	Media Player like VLC	Yes	• Audio Video Interleave • Proprietary format by Microsoft • Derivative of Resource Interchange File Format (RIFF)
RAM	Audio	RealPlayer	Yes	• Contain URLs to other RealMedia files like RM files • Developed by RealMedia
RM	Only audio or video	RealPlayer	Yes	• Used with RAM files • Stores either only audio or video or both

MPG/MPEG	Audio and video	Any media player like VLC	Yes	• Most commonly used format • Used for video and audio compression
MOV	Audio/Video	Media players like VLC	Yes	• Developed by Apple • Acts as container vor audio, video and text
ASF	Audio/Video	Media player	Yes	• Developed by Microsoft • Doesn’t specify how the audio/video must be encoded, only their structure
MID	Audio	Media player	Yes	• Part of a standard that describes a communications protocol related to musical instruments and audio devices • Small file sizes and easy to modify • Can be modified to sound like any other instrument

CONCLUSION

Thus, a sundry of file formats have been discussed above.