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

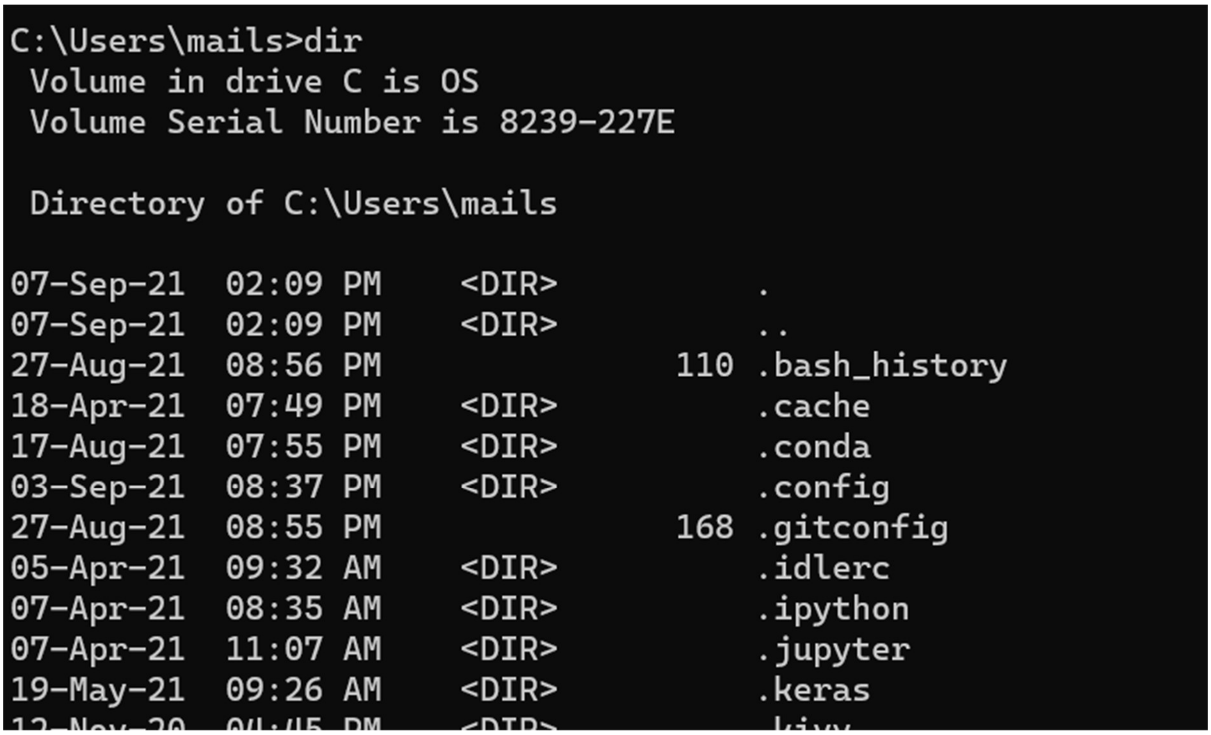
To work with the Windows Command Line.

SOME COMMANDS

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

dir

OUTPUT



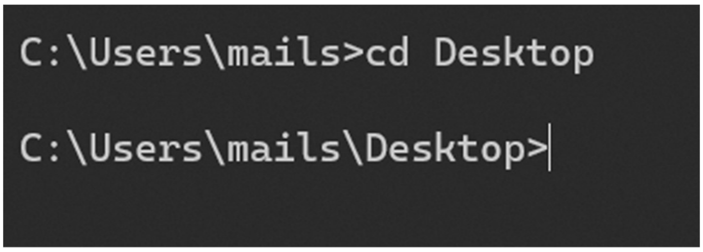
```
C:\Users\mails>dir
 Volume in drive C is OS
 Volume Serial Number is 8239-227E

 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



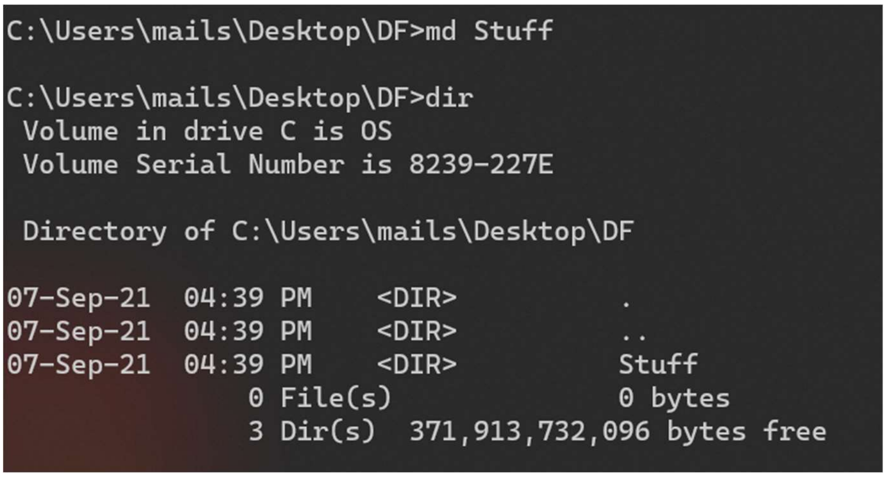
```
C:\Users\mails>cd Desktop

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

DESCRIPTION

Used to change the working directory.

md

OUTPUT



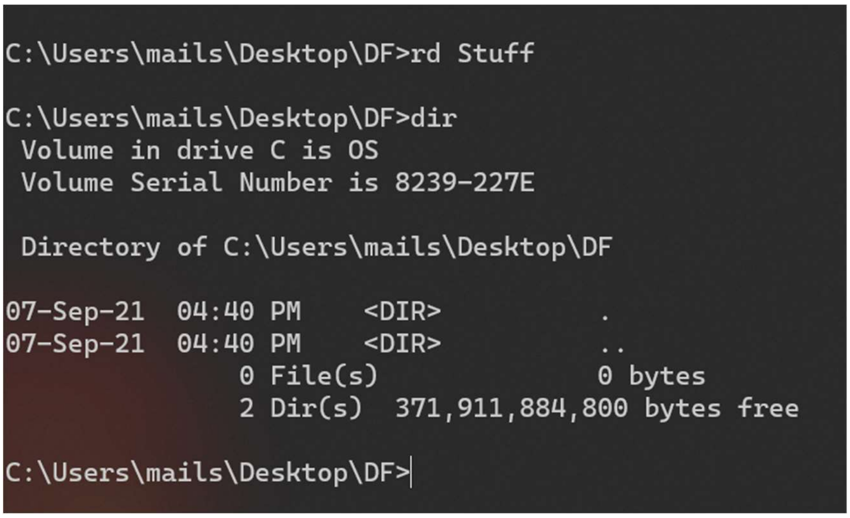
```
C:\Users\mails\Desktop\DF>md Stuff

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



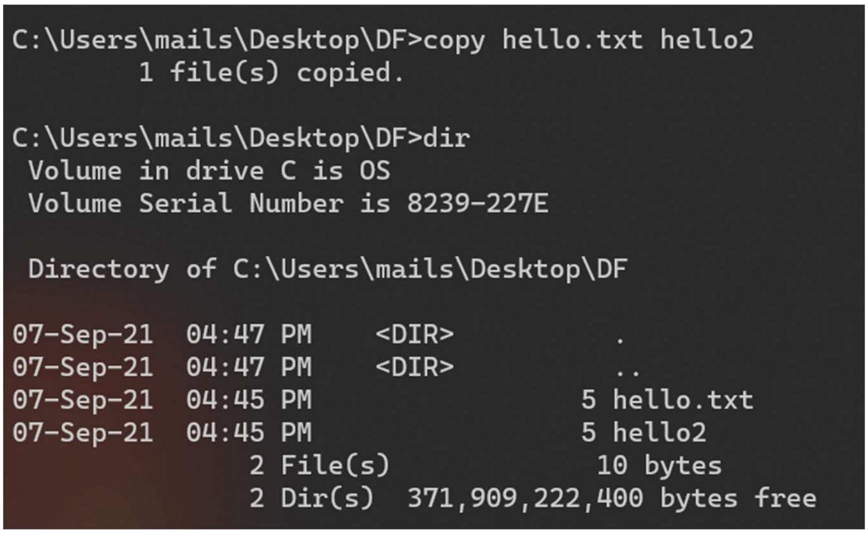
```
C:\Users\mails\Desktop\DF>rd Stuff

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



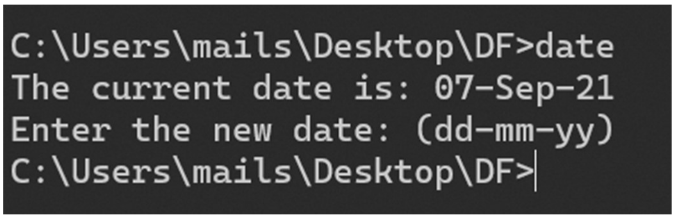
```
C:\Users\mails\Desktop\DF>copy hello.txt hello2
        1 file(s) copied.

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



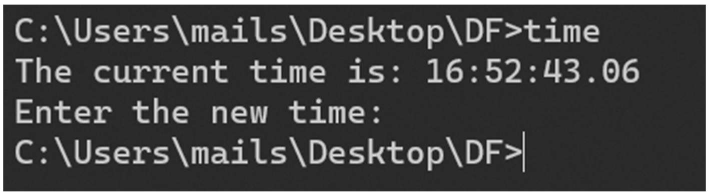
```
C:\Users\mails\Desktop\DF>date
The current date is: 07-Sep-21
Enter the new date: (dd-mm-yy)
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

Used to display and reset date.

time

OUTPUT



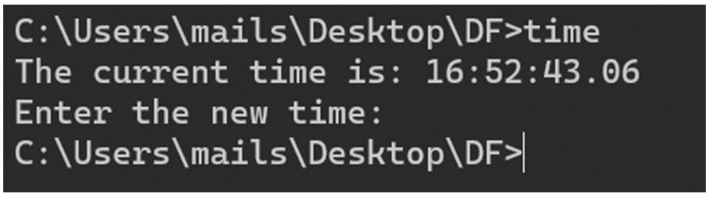
```
C:\Users\mails\Desktop\DF>time
The current time is: 16:52:43.06
Enter the new time:
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

Used to display and reset time.

vol

OUTPUT



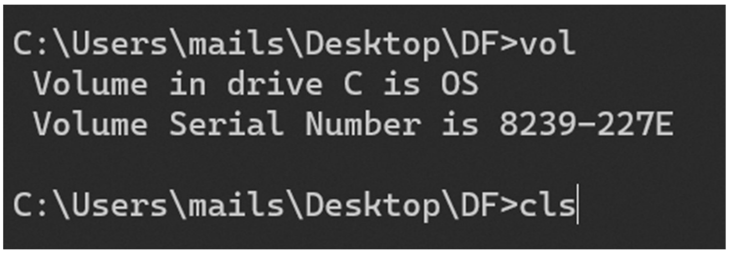
```
C:\Users\mails\Desktop\DF>time
The current time is: 16:52:43.06
Enter the new time:
C:\Users\mails\Desktop\DF>
```

DESCRIPTION

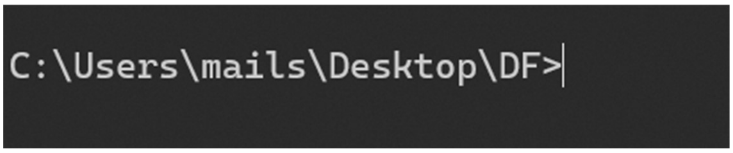
Used to display the volume label and volume serial number of a logical drive.

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
```



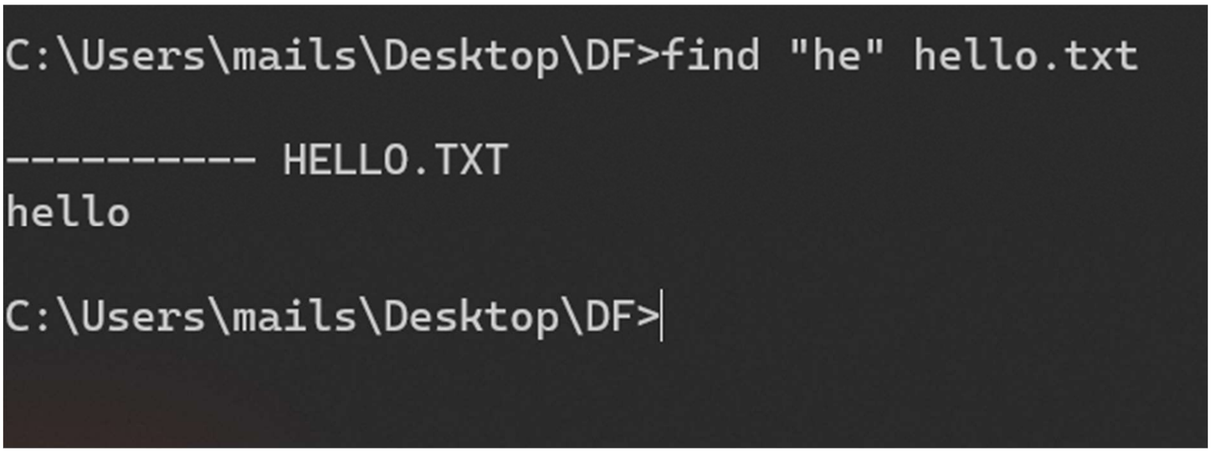
```
C:\Users\mails\Desktop\DF>
```

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

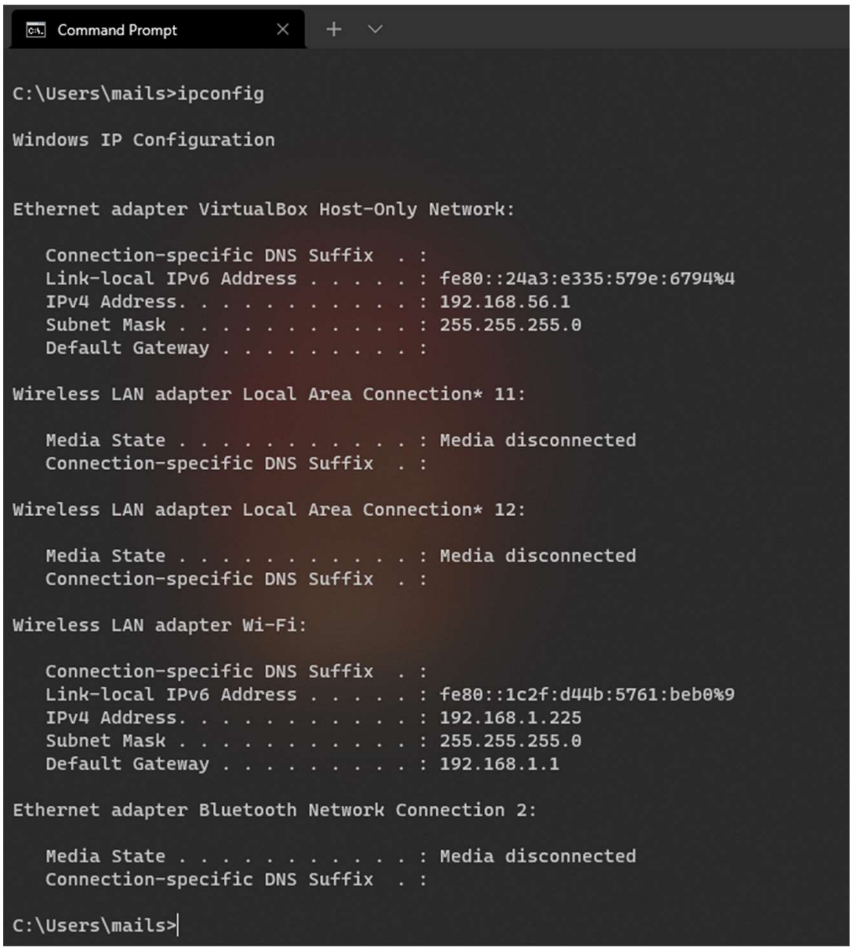
TASK 1

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

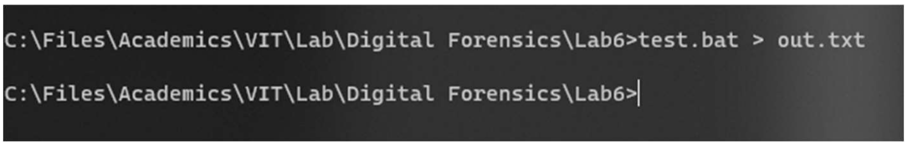
Create a batch file that will capture the following volatile information from an evidence system and store it a file.

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

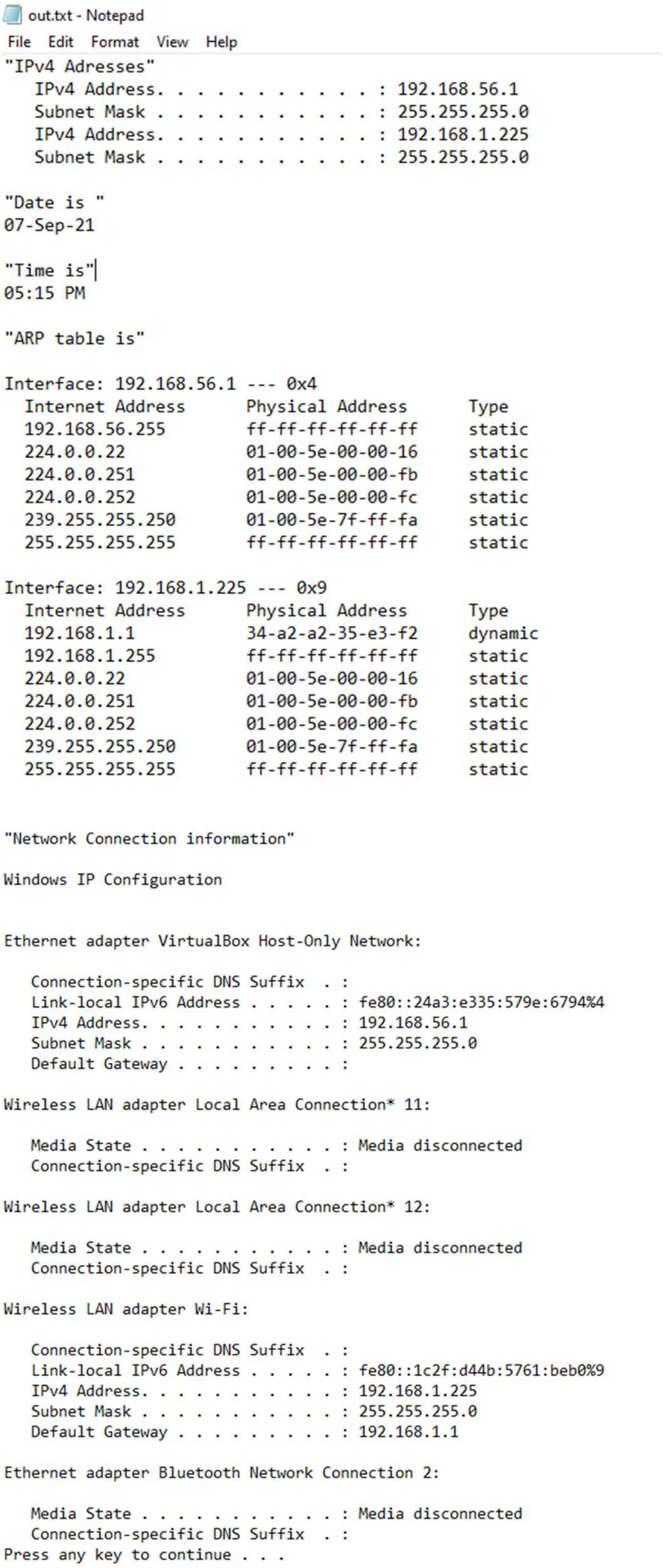
STEPS AND COMMANDS

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.