Digital Forensics - Lab 5

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

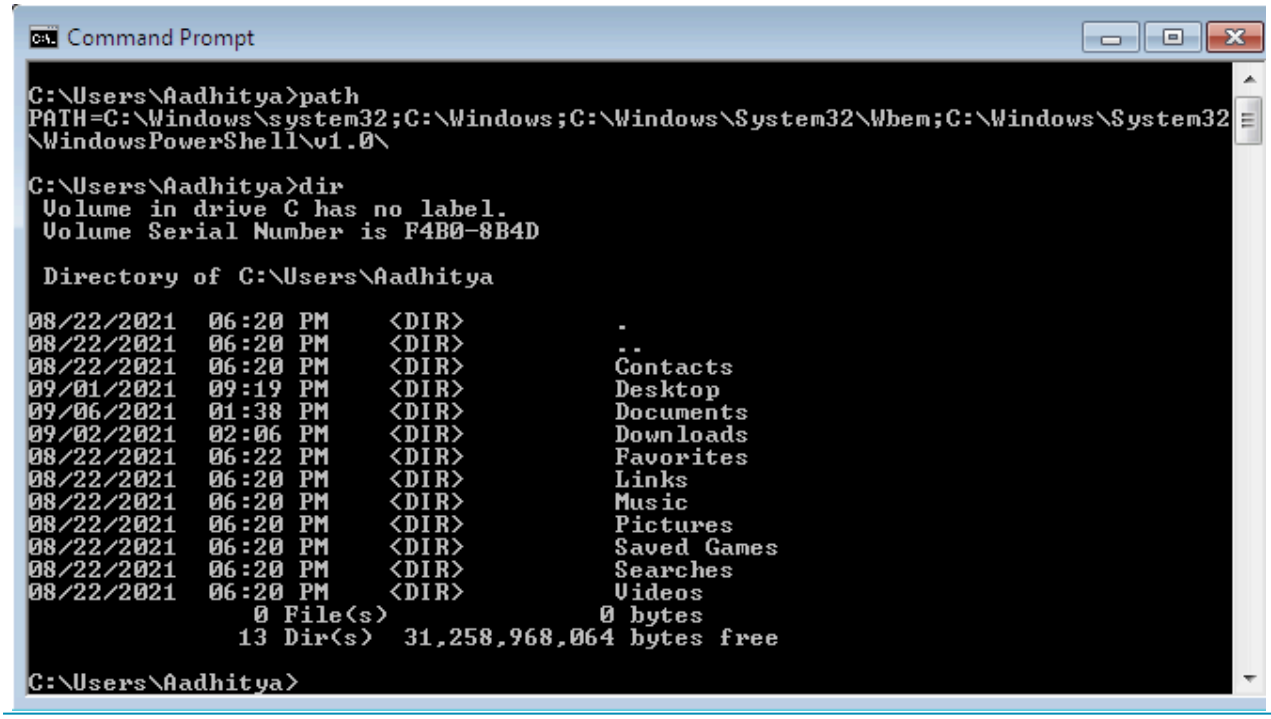
- 2 September 2021

Question 1 :

Experiment with a few basic commands using the windows command line tool, Use both internal and external commands, and show the output.

path — This command is used to display the path to the current folder in which the terminal has been opened.

dir — This command is used to list of all the files and folders in the current directory.

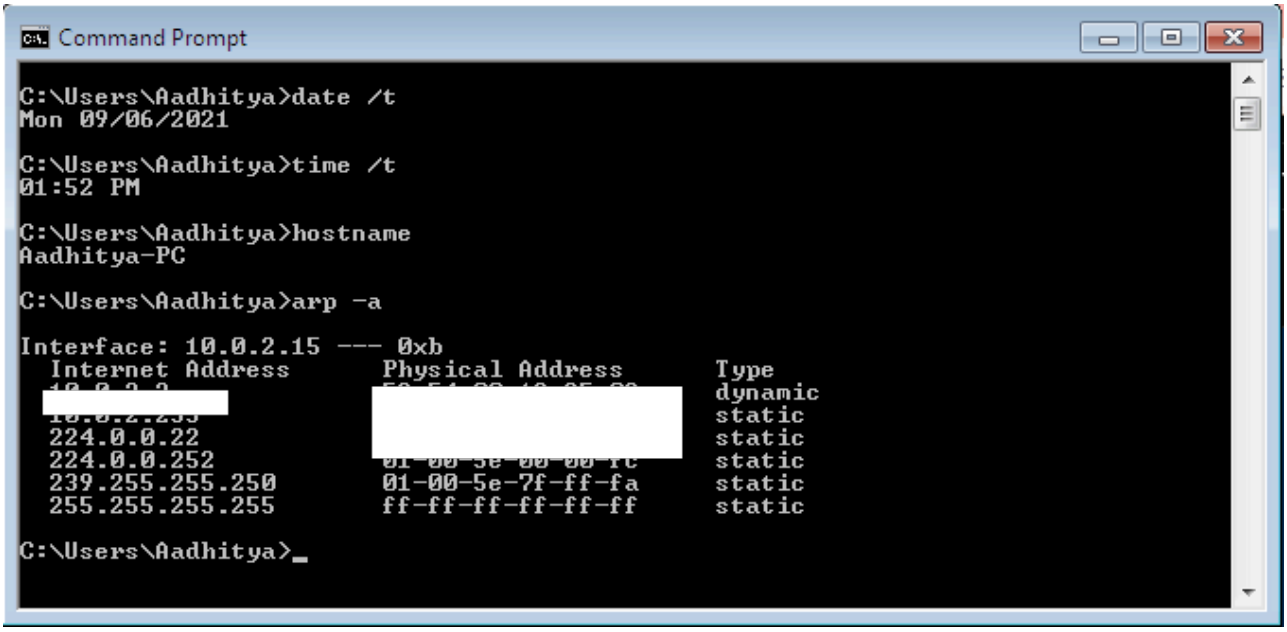


date — This command is used to display the current date in the timezone where the computer is placed.

time — This command is used to display the current time in the timezone where the computer is placed.

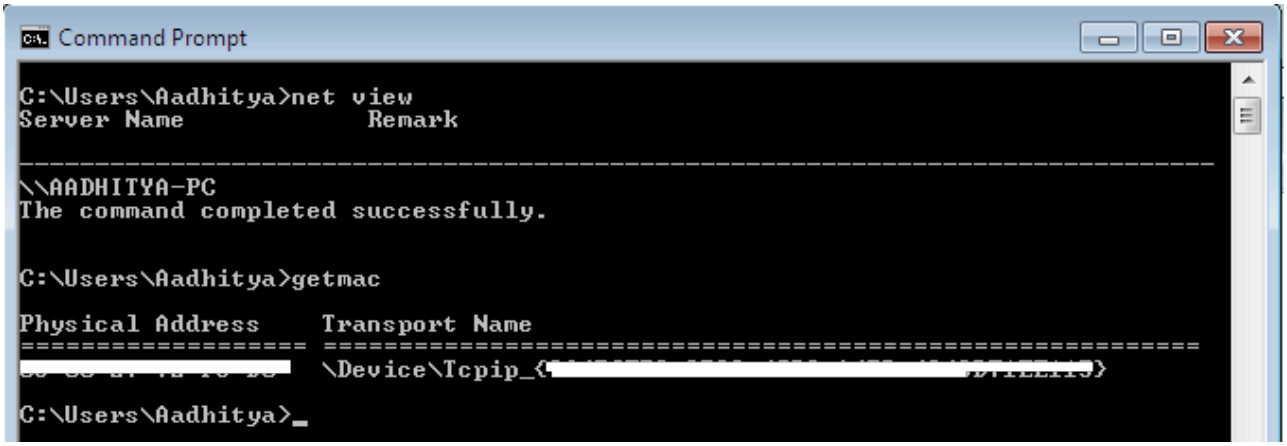
hostname — This command is used to display the hostname of the computer which is the unique name of the computer in the network in which it is connected.

arp -a — This command is used to display the Address Resolution Protocol Table. The ARP (Address Resolution Protocol) cache is a collection of ARP entries (mostly dynamic) that are created when a hostname is resolved to an IP address and then an IP address is resolved to a MAC address.



net view — This command is used to display the list of computers in the network.

getmac — This command is used to display the Mac address of the current computer.



ipconfig — This command is used to display all the network configuration of the computer when connected to a network, namely its IP address, its subnet mask, etc.

```
Command Prompt

C:\Users\Aadhitya>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

Tunnel adapter isatap.{[redacted]}:

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

C:\Users\Aadhitya>
```

```
Command Prompt

C:\Users\Aadhitya>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Aadhitya-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : [redacted]D0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : [redacted](Preferred)
   IPv4 Address. . . . . . . . . . . : [redacted]ferred)
   Subnet Mask . . . . . . . . . . . : [redacted]
   Lease Obtained. . . . . . . . . . : Monday, September 06, 2021 1:31:43 PM
   Lease Expires . . . . . . . . . . : Tuesday, September 07, 2021 1:31:41 PM
   Default Gateway . . . . . . . . . : [redacted]
   DHCP Server . . . . . . . . . . . : [redacted]
   DHCPv6 IAID . . . . . . . . . . . : [redacted]
   DHCPv6 Client DUID. . . . . . . . : [redacted]D0

   DNS Servers . . . . . . . . . . . : [redacted]
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{[redacted]15}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\Users\Aadhitya>_
```

netstat — It displays the network statistics namely how the computer communicates with other devices on the network.

```
Command Prompt

C:\Users\Aadhitya>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    [redacted]             [redacted]             ESTABLISHED
  TCP    [redacted]             [redacted]             ESTABLISHED
  TCP    [redacted]             [redacted]             ESTABLISHED
  TCP    [redacted]             [redacted]             ESTABLISHED
  TCP    [redacted]             [redacted]             ESTABLISHED
  TCP    [redacted]             [redacted]             ESTABLISHED
  TCP    127.0.0.1:49169        Aadhitya-PC:49170      ESTABLISHED
  TCP    127.0.0.1:49170        Aadhitya-PC:49169      ESTABLISHED
  TCP    127.0.0.1:49171        Aadhitya-PC:49172      ESTABLISHED
  TCP    127.0.0.1:49172        Aadhitya-PC:49171      ESTABLISHED
  TCP    127.0.0.1:49173        Aadhitya-PC:49174      ESTABLISHED
  TCP    127.0.0.1:49174        Aadhitya-PC:49173      ESTABLISHED
  TCP    127.0.0.1:49175        Aadhitya-PC:49176      ESTABLISHED
  TCP    127.0.0.1:49176        Aadhitya-PC:49175      ESTABLISHED
  TCP    127.0.0.1:49180        Aadhitya-PC:49181      ESTABLISHED
  TCP    127.0.0.1:49181        Aadhitya-PC:49180      ESTABLISHED
  TCP    127.0.0.1:49207        Aadhitya-PC:49208      ESTABLISHED
  TCP    127.0.0.1:49208        Aadhitya-PC:49207      ESTABLISHED

C:\Users\Aadhitya>_
```

```
Command Prompt

C:\Users\Aadhitya>netstat -nr
===========================================================================
Interface List
 11...[redacted]0 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.2.2       [redacted]     10
[redacted]           255.255.255.0         On-link        [redacted]    266
[redacted]       255.255.255.255         On-link        [redacted]    266
[redacted]       255.255.255.255         On-link        [redacted]    266
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link         10.0.2.15    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link         [redacted]   266
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 11    266 [redacted]               On-link
 11    266 [redacted]1/128
                                    On-link
  1    306 [redacted]               On-link
 11    266 [redacted]               On-link
===========================================================================
Persistent Routes:
  None

C:\Users\Aadhitya>_
```

ping — This command is used to ping a website, another network device, we can use this for troubleshooting the network, and also for other forensic purposes to find traces of bad actors over the network.

```
Command Prompt

C:\Users\Aadhitya>ping www.google.com

Pinging www.google.com [142.250.192.164] with 32 bytes of data:
Reply from 142.250.192.164: bytes=32 time=57ms TTL=127
Reply from 142.250.192.164: bytes=32 time=58ms TTL=127
Reply from 142.250.192.164: bytes=32 time=57ms TTL=127
Reply from 142.250.192.164: bytes=32 time=58ms TTL=127

Ping statistics for 142.250.192.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 57ms, Maximum = 58ms, Average = 57ms

C:\Users\Aadhitya>
```

We can also ping our router to get more information on our local network, in order to do this we first use the ipconfig command to know the default gateway, and then use this to ping the router for more details. It is illustrated as follows :

```
Command Prompt

C:\Users\Aadhitya>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . :
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

Tunnel adapter isatap.{                                }:

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

C:\Users\Aadhitya>ping 10.0.2.2

Pinging 10.0.2.2 with 32 bytes of data:
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Aadhitya>_
```

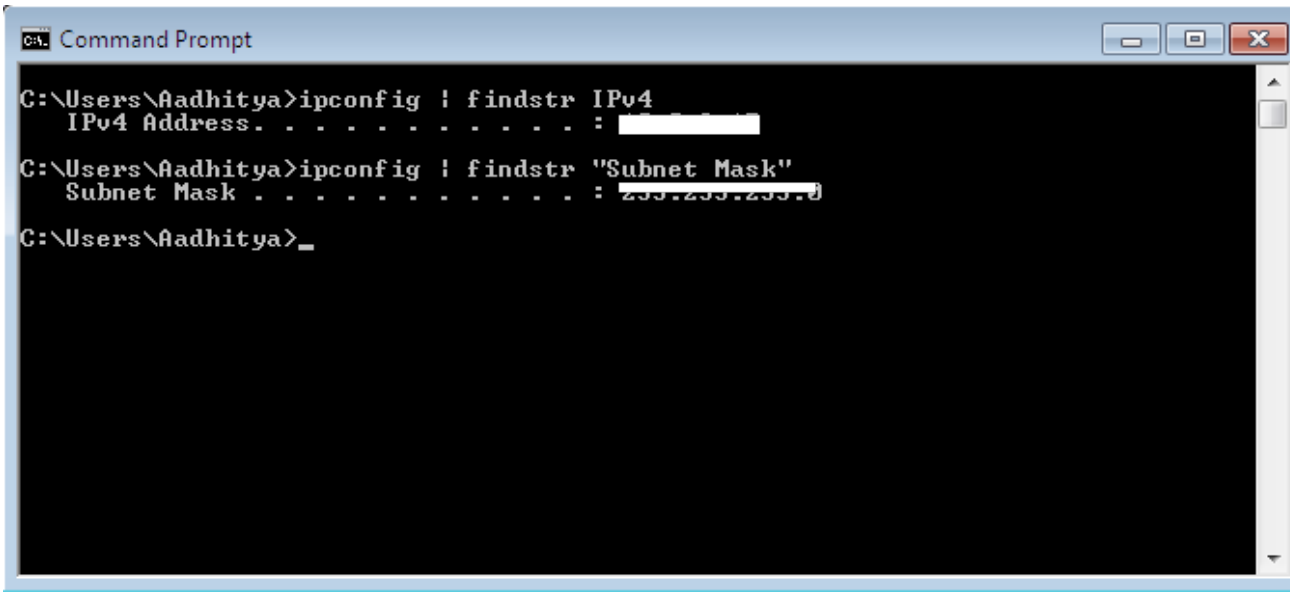
Question 2 :

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

In the previous experiment, we have observed and used multiple commands that provide many functionalities and help us in different aspects. Here in this experiment, we will modify one such tool used above and try to obtain the results from there.

The **ipconfig** command is used to know the basic network information of the computer, we the use the "**findstr"** command to search for the required portion of the output which is then displayed as the output. We thus use this combination to search for "IPv4" for the IPv4 address, and "Subnet Mask" to find the mask from the ipconfig output.

When this combination of commands are run, the outputs are as follows, where we get the IPv4 address and the subnet mask of the computer in the network :



Question 3 :

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

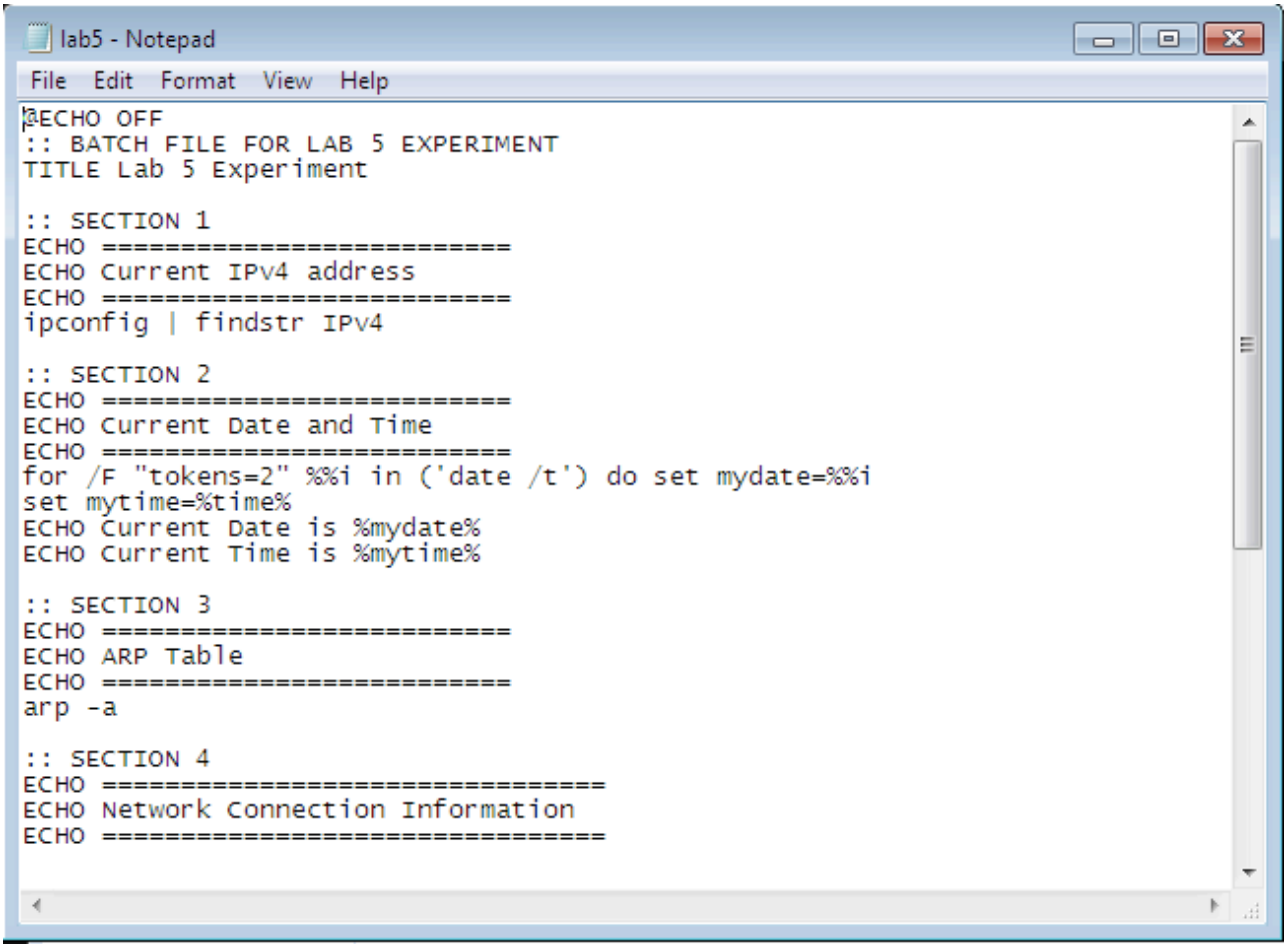
Current IPv4 address, Current date, Current time, ARP table, and the Network connection information

Take screenshots in both cases and include them in your submission.

In the above experiments, we have witnessed how commands can be run directly from inside the shell, now we shall take a look at how we can run scripts, which can be essentially a group of commands and ask the shell to run at once. This also provides higher functionalities like variables, conditional and iterative construct of statements.

In this experiment, we will write a batch script file for finding the Current IPv4 address, Current date, Current time, ARP table, and also to know the Network connection information. Many of the commands that will be used here have already been dealt with in the previous experiments, so we will proceed with writing and executing the file.

The batch file looks as follows :



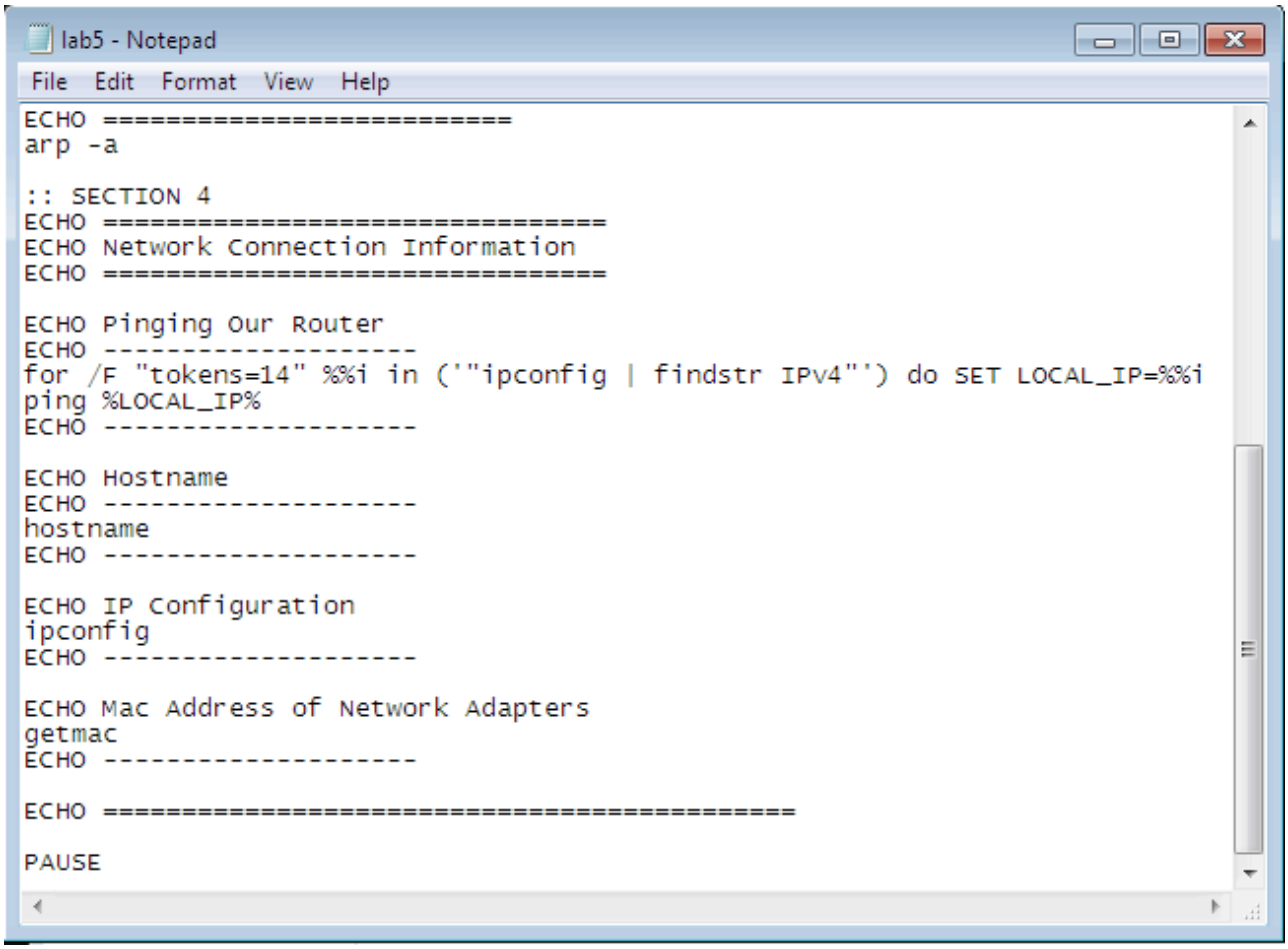

```
@ECHO OFF
:: BATCH FILE FOR LAB 5 EXPERIMENT
TITLE Lab 5 Experiment

:: SECTION 1
ECHO ==========================
ECHO Current IPv4 address
ECHO ==========================
ipconfig | findstr IPv4

:: SECTION 2
ECHO ==========================
ECHO Current Date and Time
ECHO ==========================
for /F "tokens=2" %%i in ('date /t') do set mydate=%%i
set mytime=%time%
ECHO Current Date is %mydate%
ECHO Current Time is %mytime%

:: SECTION 3
ECHO ==========================
ECHO ARP Table
ECHO ==========================
arp -a

:: SECTION 4
ECHO ================================
ECHO Network Connection Information
ECHO ================================
```




```
ECHO ==========================
arp -a

:: SECTION 4
ECHO ================================
ECHO Network Connection Information
ECHO ================================

ECHO Pinging Our Router
ECHO --------------------
for /F "tokens=14" %%i in ('"ipconfig | findstr IPv4"') do SET LOCAL_IP=%%i
ping %LOCAL_IP%
ECHO --------------------

ECHO Hostname
ECHO --------------------
hostname
ECHO --------------------

ECHO IP Configuration
ipconfig
ECHO --------------------

ECHO Mac Address of Network Adapters
getmac
ECHO --------------------

ECHO ============================================

PAUSE
```

The **PAUSE** command in the final line is used to hold the output terminal until we would like to exit, if this is absent, then the output window will close in an instant.

When executed, a new window similar to the command line opens, with the title that we have mentioned, and it displays all the outputs of all the mentioned commands, which in this case also includes some formatting to get a better understanding of the output.

The output when this is executed is as follows :

Lab 5 Experiment

```
==========================
Current IPv4 address
==========================
   IPv4 Address. . . . . . . . . . . : 10[redacted]
==========================
Current Date and Time
==========================
Current Date is 09/06/2021
Current Time is 14:17:52.31
==========================
ARP Table
==========================

Interface: 10.0.2.15 --- 0xb
  Internet Address      Physical Address      Type
  10.0.2.2              52[redacted]-02       dynamic
  [redacted]            ff[redacted]-ff       static
                        01[redacted]-16       static
                        01[redacted]-fc       static
                        01[redacted]-fa       static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
===================================
Network Connection Information
===================================
Pinging Our Router
--------------------

Pinging [redacted] with 32 bytes of data:
Reply from [redacted]: bytes=32 time<1ms TTL=128
Reply from [redacted]: bytes=32 time<1ms TTL=128
Reply from [redacted]: bytes=32 time<1ms TTL=128
Reply from [redacted]15: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
--------------------
```

Lab 5 Experiment

```
--------------------
Hostname
--------------------
Aadhitya-PC
--------------------
IP Configuration

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : f[redacted]
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : [redacted]
   Default Gateway . . . . . . . . . : [redacted]

Tunnel adapter isatap.{[redacted]-4948D[redacted]115}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
--------------------
Mac Address of Network Adapters

Physical Address    Transport Name
=================== ==============================================================
[redacted]00        \Device\Tcpip_{964[redacted]115}
--------------------
==========================================
Press any key to continue . . .
```

CONCLUSION

In this lab experiments, we have dealt with and seen how the command line tools and the shell commands are run, a few examples of how powerful they are, and also seen how such commands can be grouped together and executed at once like executing scripts using batch files which provide useful functionalities for the ease of forensic analysis.

REFERENCES

- https://www.digitalcitizen.life/command-prompt-advanced-networking-commands/
- https://www.windowscentral.com/how-create-and-run-batch-file-windows-10
- https://stackoverflow.com/questions/5898763/how-do-i-get-the-ip-address-into-a-batch-file-variable
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands