**Lab 6**

**R. Harini**

**18BCE1010**

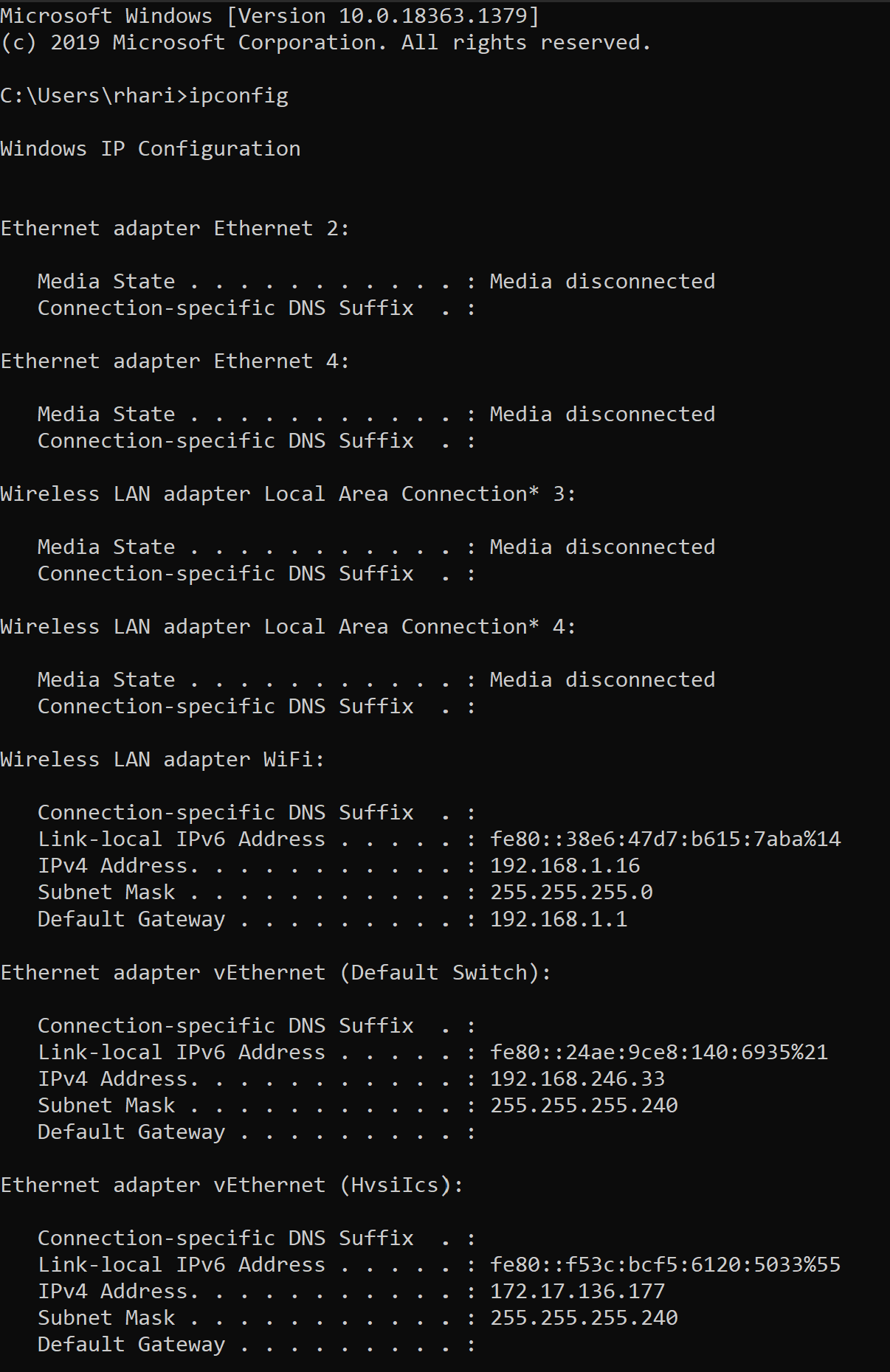
**Aim:** To become familiar with the Windows command line for digital forensics investigations

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

**Procedure:** Using ipconfig command

IPv4: 172.17.136.177

Subnet mask: 255.255.255.240

****

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

**Code:**

@echo off

FOR /F "delims=: tokens=2" %%a in ('ipconfig ^| find "IPv4"') do set \_IPAddress=%%a

ECHO IP address is: %\_IPAddress% >> grv.txt

For /f "tokens=2-4 delims=/ " %%a in ('date /t') do (set mydate=%%c-%%a-%%b)

For /f "tokens=1-2 delims=/:" %%a in ('time /t') do (set mytime=%%a%%b)

echo Date: %mydate% >>grv.txt

echo Time: %mytime% >>grv.txt

echo. >>grv.txt

echo ARP Table >>grv.txt

FOR /L %%A IN (1,1,5) DO (

arp -a | findstr 20-7c-8f-3f-03-9c

cls

if %errorlevel% GEQ 1 (

echo The device is offline

Echo Device is offline at %time% on %date%. >> grv.txt

) else (

echo The device is online.

Echo Device is online at %time% on %date%. >> grv.txt

)

timeout 3 >nul /nobreak

)

echo. >>grv.txt

echo Network Connection Information >>grv.txt

netstat -a>>grv.txt

**Screenshot**

