

**Name: Ashish Das**

**Reg. No.: 19BCE1160**

**Faculty: Nagraj S. V.**

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

```
Command Prompt
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::a9c5:7b4c:459:fe20%6
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 3:

    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::6d99:7884:7691:a5bc%22
    IPv4 Address. . . . . : 192.168.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\Ashish Das>
```

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

```
@echo off

echo Exercise 5 - 19BCE1160>output.txt
echo.>>output.txt

set ip_address_string="IPv4 Address"
for /f "usebackq tokens=2 delims=" %%f in (`ipconfig ^| findstr /c:%ip_address_string`) do echo IPv4 Address: %%f>>output.txt

echo.>>output.txt
echo Current Date: %date%>>output.txt
echo Current Time: %time%>>output.txt

echo.>>output.txt
echo ARP Table:>>output.txt
for /f "delims=" %%f in ('arp -a') do echo %%f>>output.txt

echo.>>output.txt
echo Network connection information:>>output.txt
for /f "delims=" %%f in ('netstat -n') do echo %%f>>output.txt
```

```
2
3 IPv4 Address: 192.168.56.1
4 IPv4 Address: 192.168.253.170
5
6 Current Date: Mon 09/06/2021
7 Current Time: 22:50:04.80
8
9 ARP Table:
10 Interface: 192.168.253.170 --- 0x6
11 Internet Address    Physical Address      Type
12 192.168.253.50      06-53-00-00-00-00    dynamic
13 192.168.253.255     ff-ff-ff-ff-ff-ff    static
14 224.0.0.22          01-00-5e-00-00-00    static
15 224.0.0.251         01-00-5e-00-00-00    static
16 224.0.0.252         01-00-5e-00-00-00    static
17 239.255.255.250     01-00-5e-00-00-00    static
18 255.255.255.255     ff-ff-ff-ff-ff-ff    static
19 Interface: 192.168.56.1 --- 0x1a
20 Internet Address    Physical Address      Type
21 192.168.56.255      ff-ff-ff-ff-ff-ff    static
22 224.0.0.22          01-00-5e-00-00-00    static
23 224.0.0.251         01-00-5e-00-00-00    static
24 224.0.0.252         01-00-5e-00-00-00    static
25 239.255.255.250     01-00-5e-00-00-00    static
26
27 Network connection information:
28 Active Connections
29 Proto local Address          Foreign Address         State
30 TCP    127.0.0.1:1043          127.0.0.1:1044          ESTABLISHED
31 TCP    127.0.0.1:1043          127.0.0.1:1047          ESTABLISHED
32 TCP    127.0.0.1:1044          127.0.0.1:1043          ESTABLISHED
33 TCP    127.0.0.1:1045          127.0.0.1:19012         ESTABLISHED
34 TCP    127.0.0.1:1046          127.0.0.1:19487         ESTABLISHED
35 TCP    127.0.0.1:1047          127.0.0.1:1043          ESTABLISHED
36 TCP    127.0.0.1:19012         127.0.0.1:1045          ESTABLISHED
37 TCP    127.0.0.1:19487         127.0.0.1:1046          ESTABLISHED
38 TCP    192.168.253.170:1024    115.240.194.4:443       CLOSE_WAIT
39 TCP    192.168.253.170:1025    151.101.1.69:443        ESTABLISHED
40 TCP    192.168.253.170:1026    35.165.106.175:443      ESTABLISHED
41
42 C:\Users\josh\Desktop>ipconfig /all
```

