Name – Kulvir Singh

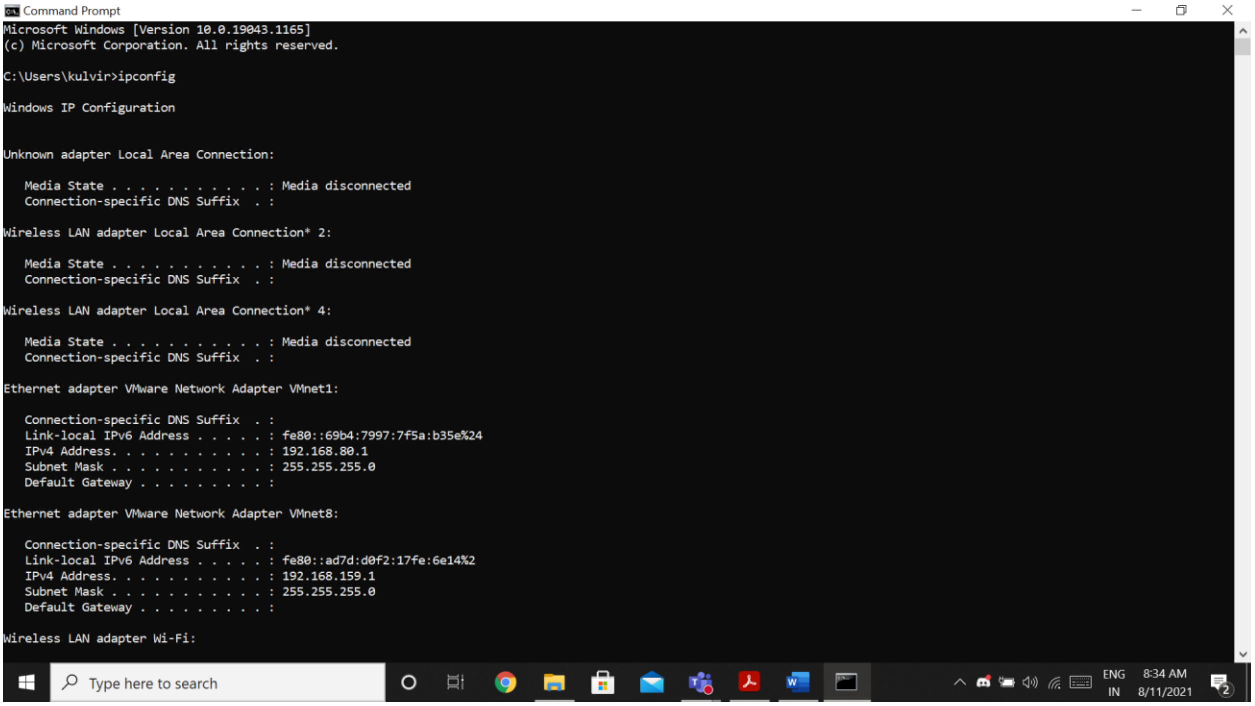
Reg. No. – 19BCE2074

Information Security and Audit Analysis Lab DA 1

COMMANDS

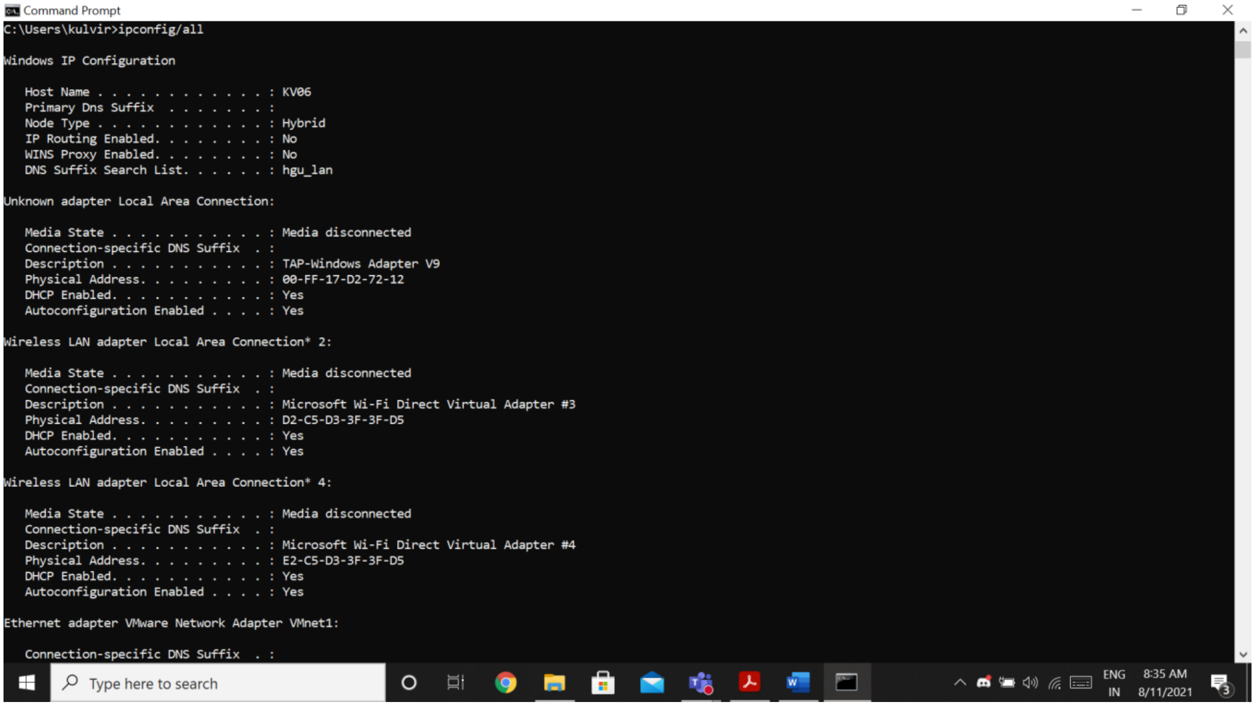
(This section has windows based commands used for investigating and configuring the computer network.)

ipconfig



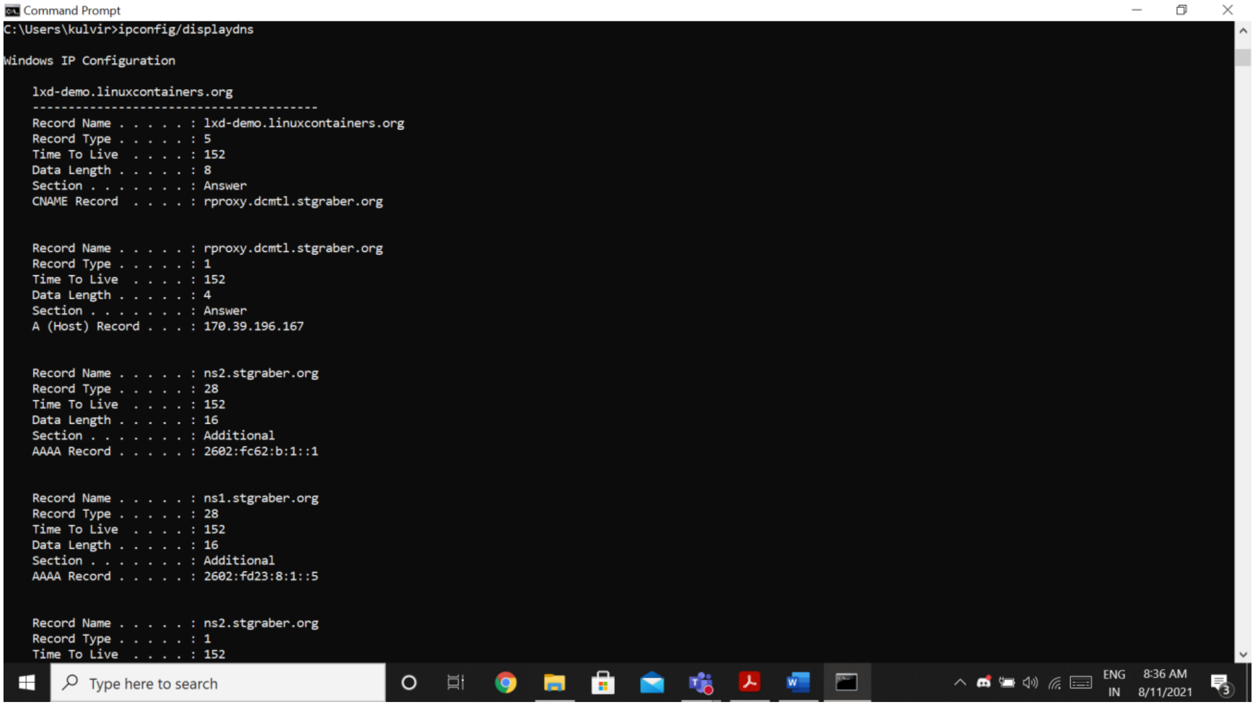
```
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kulvir>ipconfig

Windows IP Configuration


Unknown adapter Local Area Connection:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Local Area Connection* 4:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::69b4:7997:7f5a:b35e%24
   IPv4 Address. . . . . . . . . . . : 192.168.80.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ad7d:d0f2:17fe:6e14%2
   IPv4 Address. . . . . . . . . . . : 192.168.159.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:
```

ipconfig/all



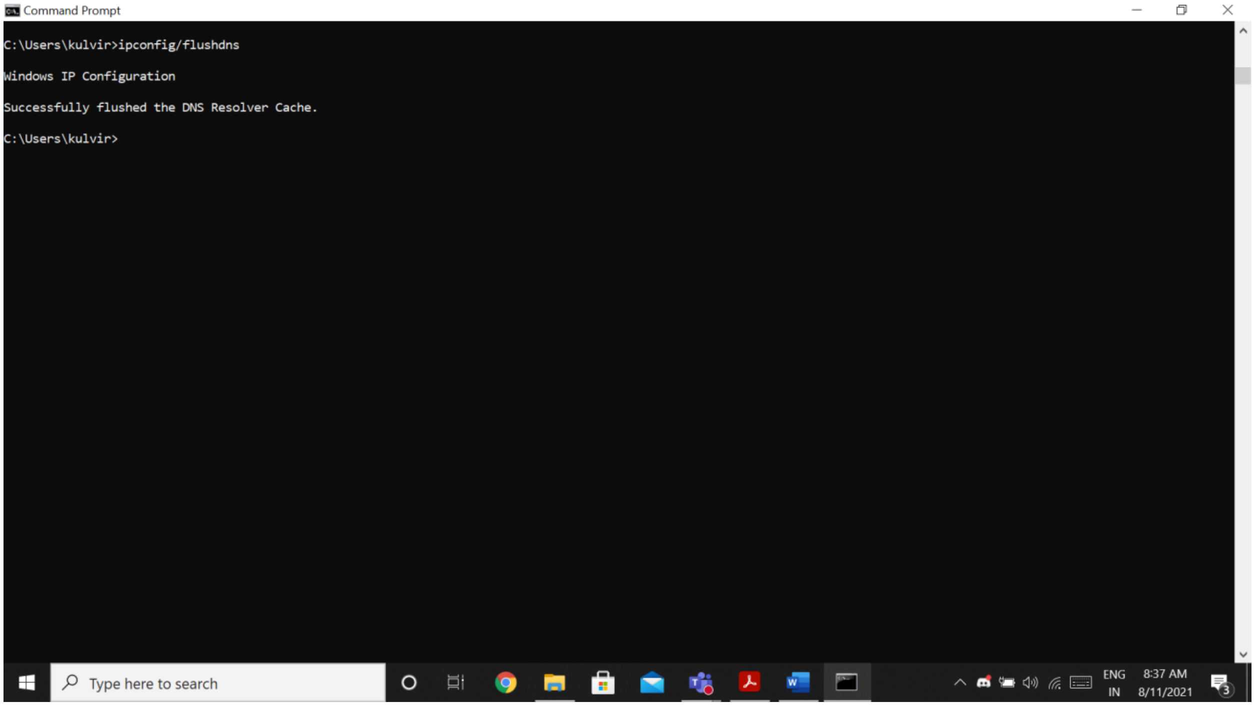
```
C:\Users\kulvir>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : KV06
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : hgu_lan

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9
   Physical Address. . . . . . . . . : 00-FF-17-D2-72-12
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : D2-C5-D3-3F-3F-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : E2-C5-D3-3F-3F-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
```

ipconfig/displaydns



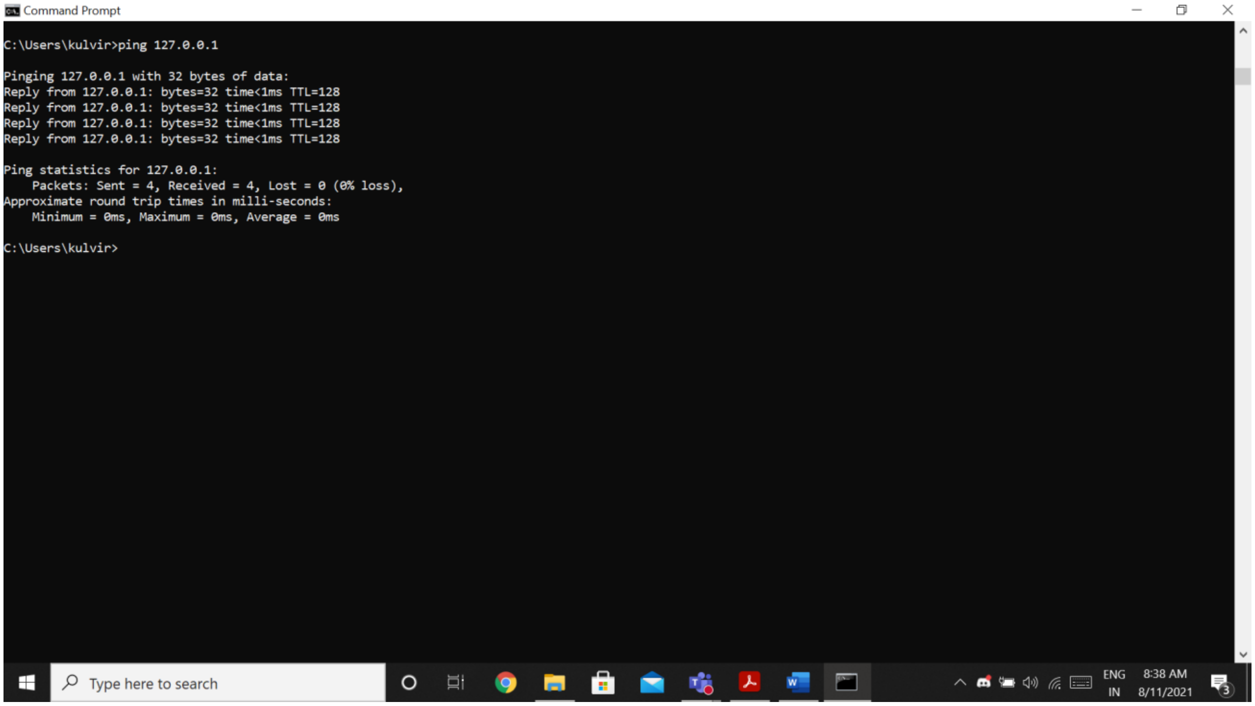
```
C:\Users\kulvir>ipconfig/displaydns

Windows IP Configuration

    lxd-demo.linuxcontainers.org
    ----------------------------------------
    Record Name . . . . . : lxd-demo.linuxcontainers.org
    Record Type . . . . . : 5
    Time To Live  . . . . : 152
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : rproxy.dcmtl.stgraber.org


    Record Name . . . . . : rproxy.dcmtl.stgraber.org
    Record Type . . . . . : 1
    Time To Live  . . . . : 152
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 170.39.196.167


    Record Name . . . . . : ns2.stgraber.org
    Record Type . . . . . : 28
    Time To Live  . . . . : 152
    Data Length . . . . . : 16
    Section . . . . . . . : Additional
    AAAA Record . . . . . : 2602:fc62:b:1::1


    Record Name . . . . . : ns1.stgraber.org
    Record Type . . . . . : 28
    Time To Live  . . . . : 152
    Data Length . . . . . : 16
    Section . . . . . . . : Additional
    AAAA Record . . . . . : 2602:fd23:8:1::5


    Record Name . . . . . : ns2.stgraber.org
    Record Type . . . . . : 1
    Time To Live  . . . . : 152
```

ipconfig/flushdns

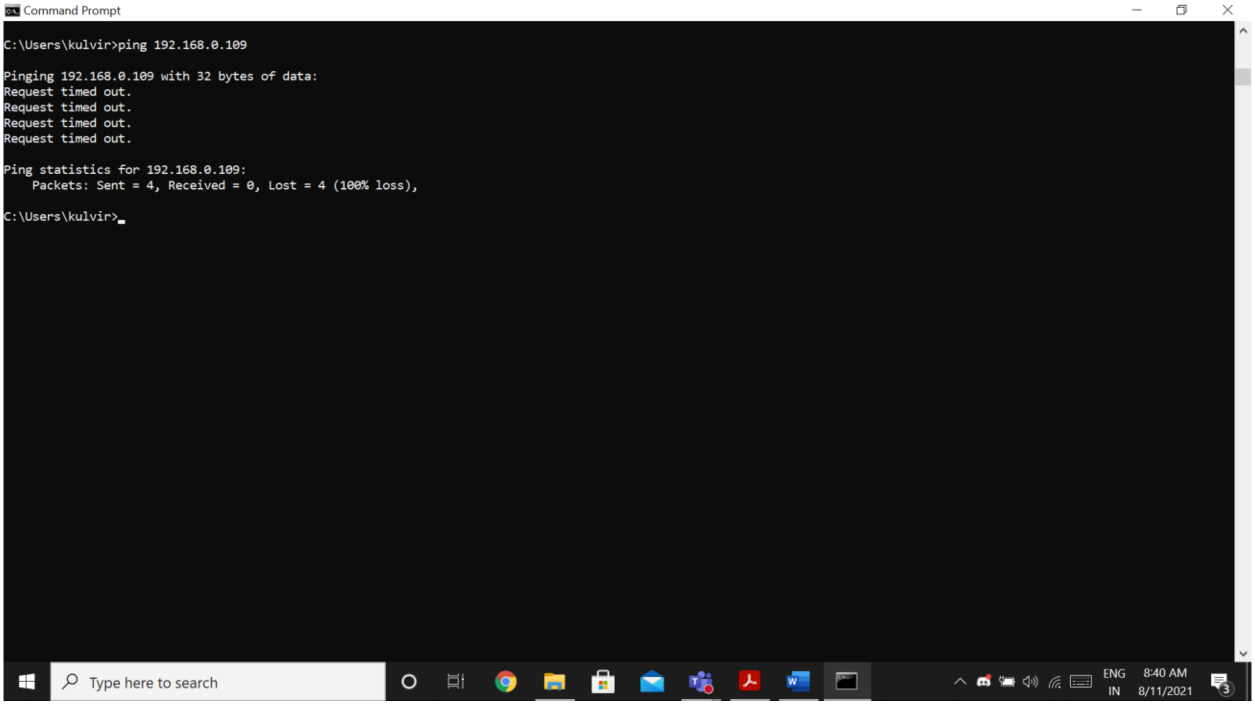


```
C:\Users\kulvir>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\kulvir>
```

ping

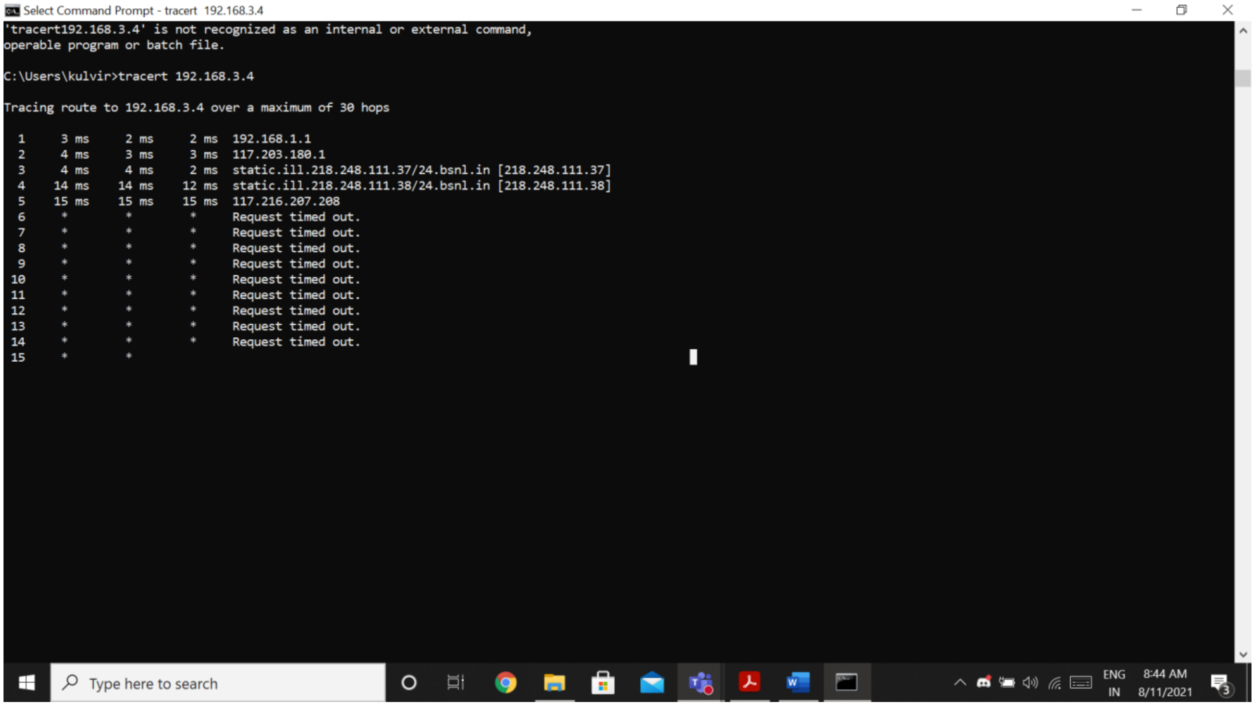


```
C:\Users\kulvir>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\kulvir>
```



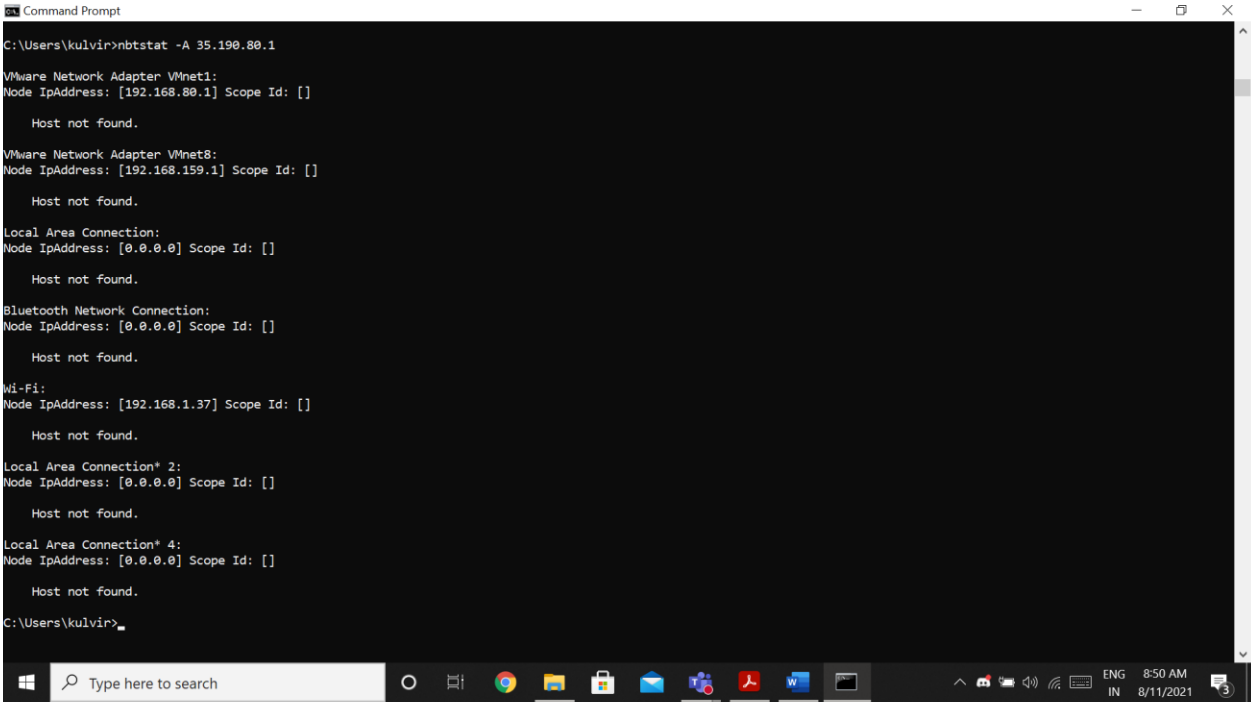
```
C:\Users\kulvir>ping 192.168.0.109

Pinging 192.168.0.109 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.109:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\kulvir>_
```

tracert



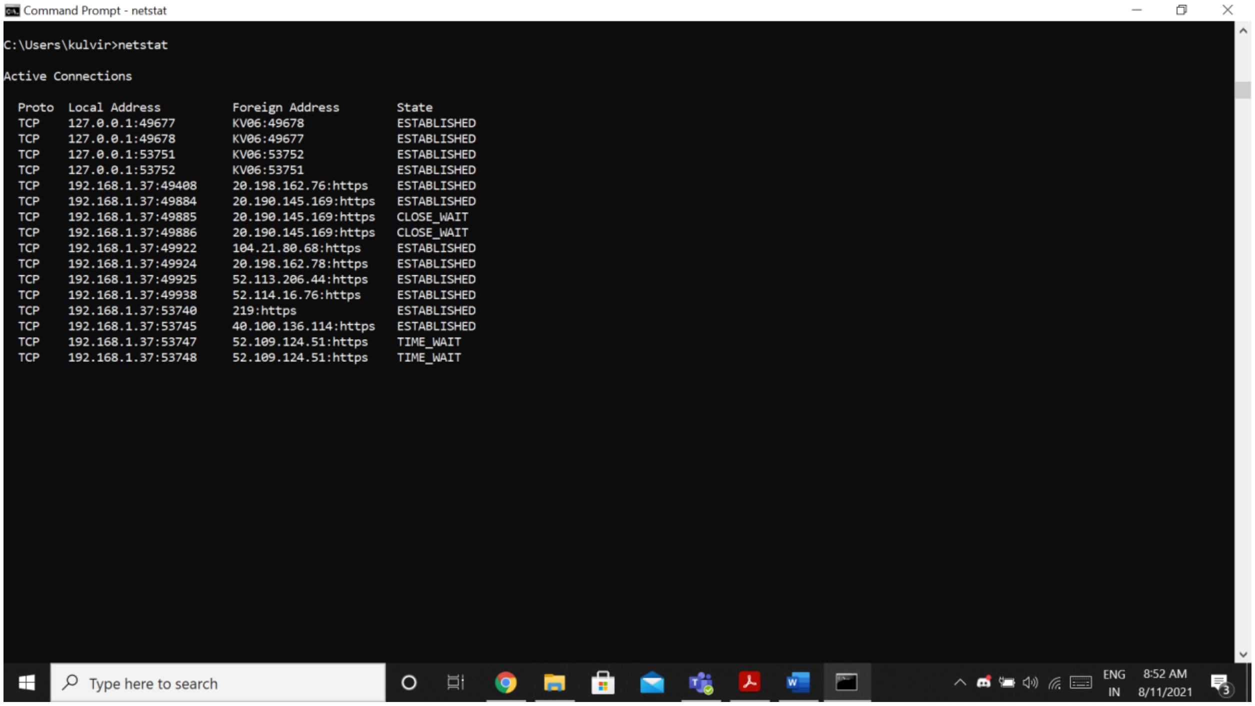
```
'tracert192.168.3.4' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\kulvir>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops

  1     3 ms     2 ms     2 ms  192.168.1.1
  2     4 ms     3 ms     3 ms  117.203.180.1
  3     4 ms     4 ms     2 ms  static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]
  4    14 ms    14 ms    12 ms  static.ill.218.248.111.38/24.bsnl.in [218.248.111.38]
  5    15 ms    15 ms    15 ms  117.216.207.208
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *
```

nbtstat



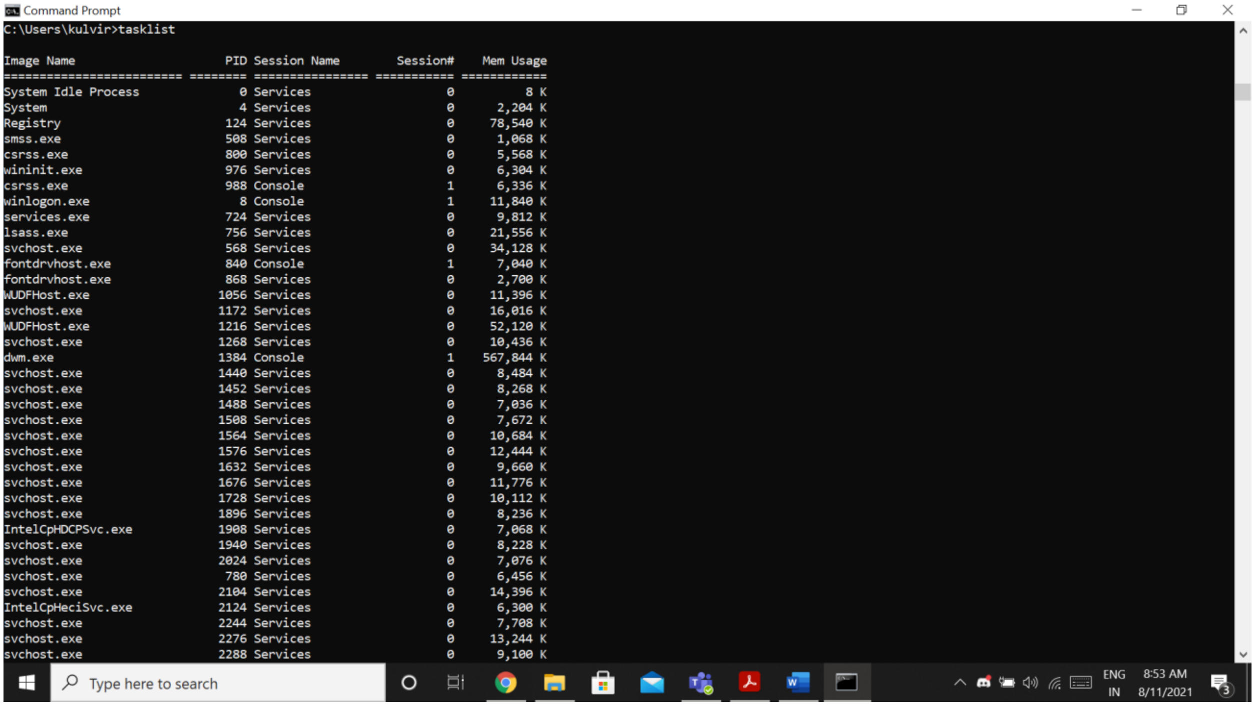
```
C:\Users\kulvir>nbtstat -A 35.190.80.1

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.80.1] Scope Id: []

    Host not found.

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.159.1] Scope Id: []

    Host not found.

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Wi-Fi:
Node IpAddress: [192.168.1.37] Scope Id: []

    Host not found.

Local Area Connection* 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

Local Area Connection* 4:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

C:\Users\kulvir>_
```

netstat



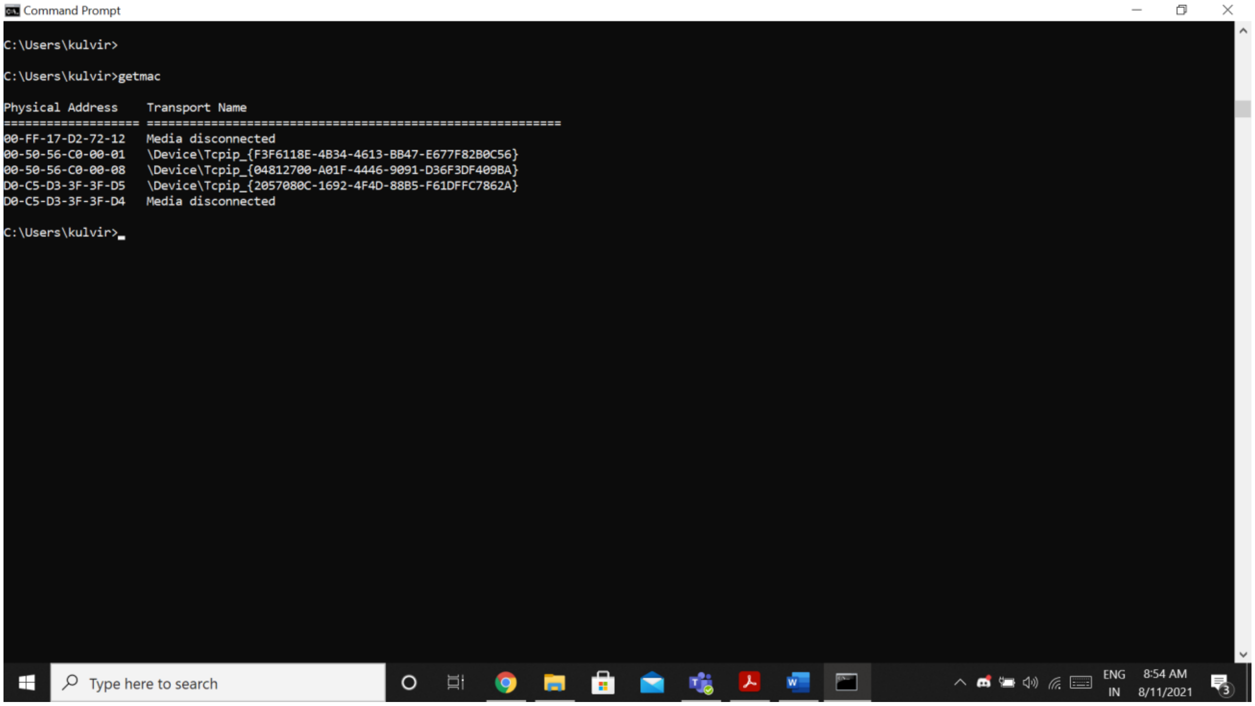
```
C:\Users\kulvir>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49677        KV06:49678             ESTABLISHED
  TCP    127.0.0.1:49678        KV06:49677             ESTABLISHED
  TCP    127.0.0.1:53751        KV06:53752             ESTABLISHED
  TCP    127.0.0.1:53752        KV06:53751             ESTABLISHED
  TCP    192.168.1.37:49408     20.198.162.76:https    ESTABLISHED
  TCP    192.168.1.37:49884     20.190.145.169:https   ESTABLISHED
  TCP    192.168.1.37:49885     20.190.145.169:https   CLOSE_WAIT
  TCP    192.168.1.37:49886     20.190.145.169:https   CLOSE_WAIT
  TCP    192.168.1.37:49922     104.21.80.68:https     ESTABLISHED
  TCP    192.168.1.37:49924     20.198.162.78:https    ESTABLISHED
  TCP    192.168.1.37:49925     52.113.206.44:https    ESTABLISHED
  TCP    192.168.1.37:49938     52.114.16.76:https     ESTABLISHED
  TCP    192.168.1.37:53740     219:https              ESTABLISHED
  TCP    192.168.1.37:53745     40.100.136.114:https   ESTABLISHED
  TCP    192.168.1.37:53747     52.109.124.51:https    TIME_WAIT
  TCP    192.168.1.37:53748     52.109.124.51:https    TIME_WAIT
```

tasklist



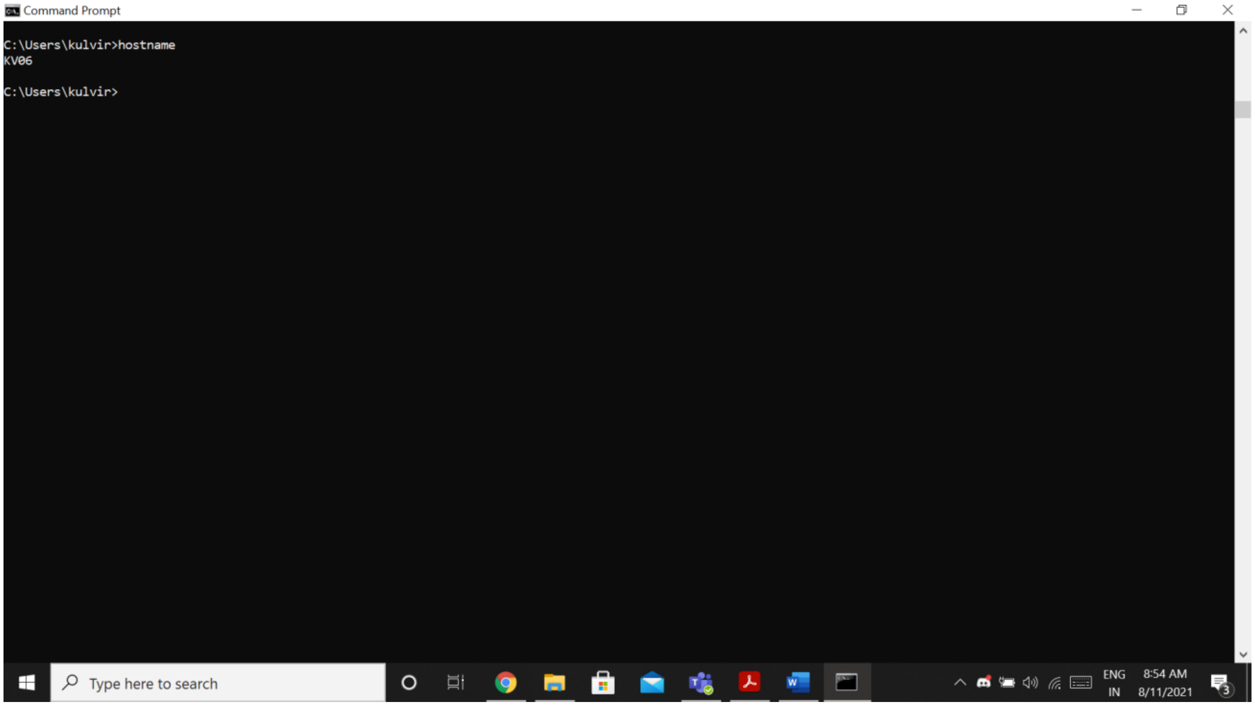
```
C:\Users\kulvir>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      2,204 K
Registry                       124 Services                   0     78,540 K
smss.exe                       508 Services                   0      1,068 K
csrss.exe                      800 Services                   0      5,568 K
wininit.exe                    976 Services                   0      6,304 K
csrss.exe                      988 Console                    1      6,336 K
winlogon.exe                     8 Console                    1     11,840 K
services.exe                   724 Services                   0      9,812 K
lsass.exe                      756 Services                   0     21,556 K
svchost.exe                    568 Services                   0     34,128 K
fontdrvhost.exe                840 Console                    1      7,040 K
fontdrvhost.exe                868 Services                   0      2,700 K
WUDFHost.exe                  1056 Services                   0     11,396 K
svchost.exe                   1172 Services                   0     16,016 K
WUDFHost.exe                  1216 Services                   0     52,120 K
svchost.exe                   1268 Services                   0     10,436 K
dwm.exe                       1384 Console                    1    567,844 K
svchost.exe                   1440 Services                   0      8,484 K
svchost.exe                   1452 Services                   0      8,268 K
svchost.exe                   1488 Services                   0      7,036 K
svchost.exe                   1508 Services                   0      7,672 K
svchost.exe                   1564 Services                   0     10,684 K
svchost.exe                   1576 Services                   0     12,444 K
svchost.exe                   1632 Services                   0      9,660 K
svchost.exe                   1676 Services                   0     11,776 K
svchost.exe                   1728 Services                   0     10,112 K
svchost.exe                   1896 Services                   0      8,236 K
IntelCpHDCPSvc.exe            1908 Services                   0      7,068 K
svchost.exe                   1940 Services                   0      8,228 K
svchost.exe                   2024 Services                   0      7,076 K
svchost.exe                    780 Services                   0      6,456 K
svchost.exe                   2104 Services                   0     14,396 K
IntelCpHeciSvc.exe            2124 Services                   0      6,300 K
svchost.exe                   2244 Services                   0      7,708 K
svchost.exe                   2276 Services                   0     13,244 K
svchost.exe                   2288 Services                   0      9,100 K
```

getmac



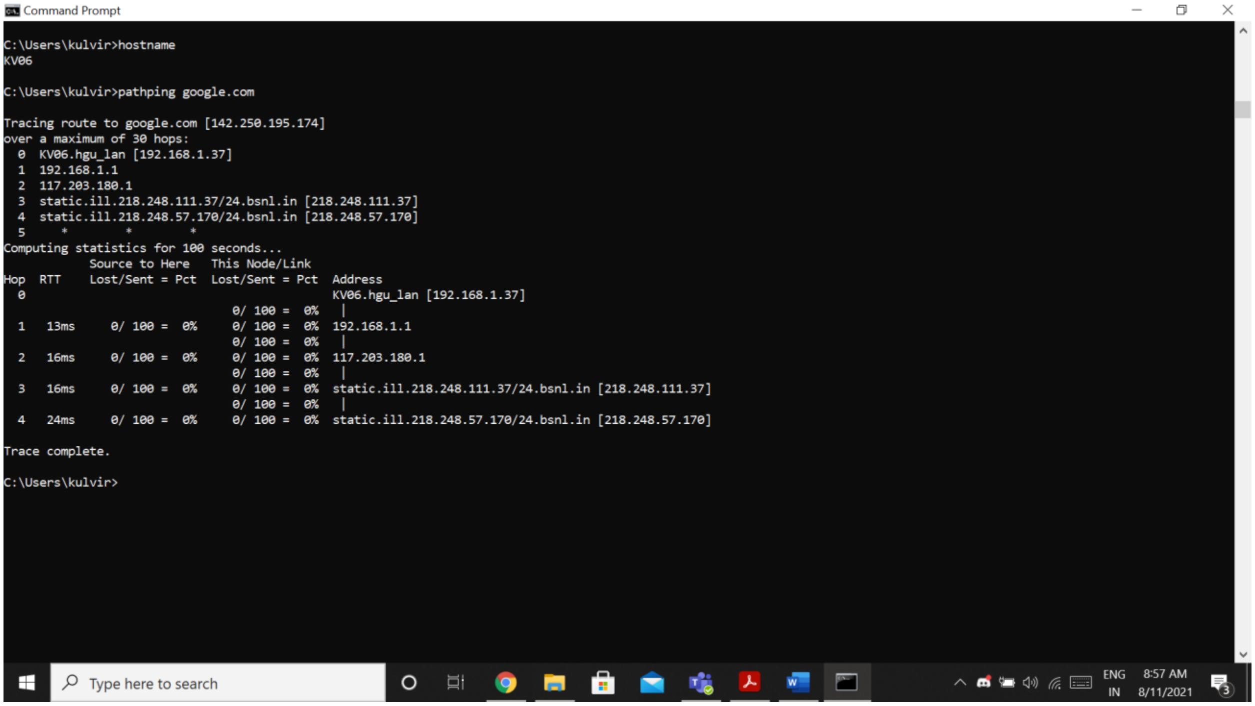
```
C:\Users\kulvir>

C:\Users\kulvir>getmac

Physical Address    Transport Name
=================== ==========================================================
00-FF-17-D2-72-12   Media disconnected
00-50-56-C0-00-01   \Device\Tcpip_{F3F6118E-4B34-4613-BB47-E677F82B0C56}
00-50-56-C0-00-08   \Device\Tcpip_{04812700-A01F-4446-9091-D36F3DF409BA}
D0-C5-D3-3F-3F-D5   \Device\Tcpip_{2057080C-1692-4F4D-88B5-F61DFFC7862A}
D0-C5-D3-3F-3F-D4   Media disconnected

C:\Users\kulvir>_
```

hostname



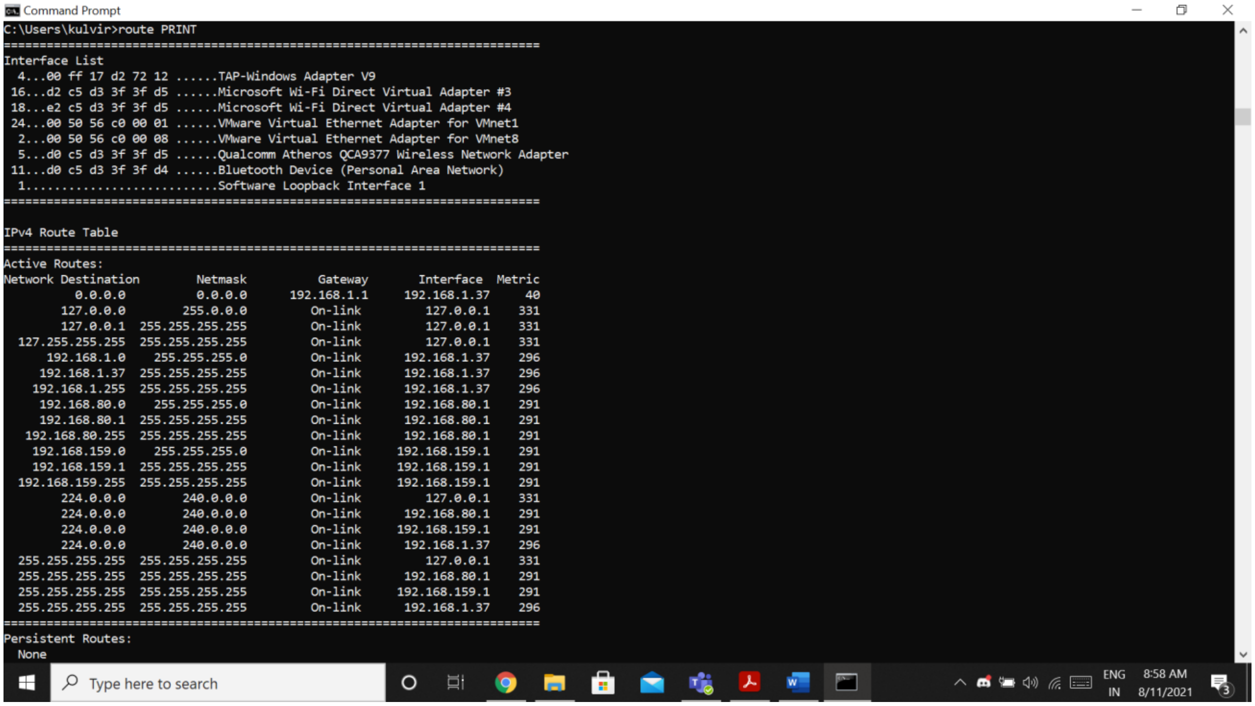
```
C:\Users\kulvir>hostname
KV06

C:\Users\kulvir>
```

pathping



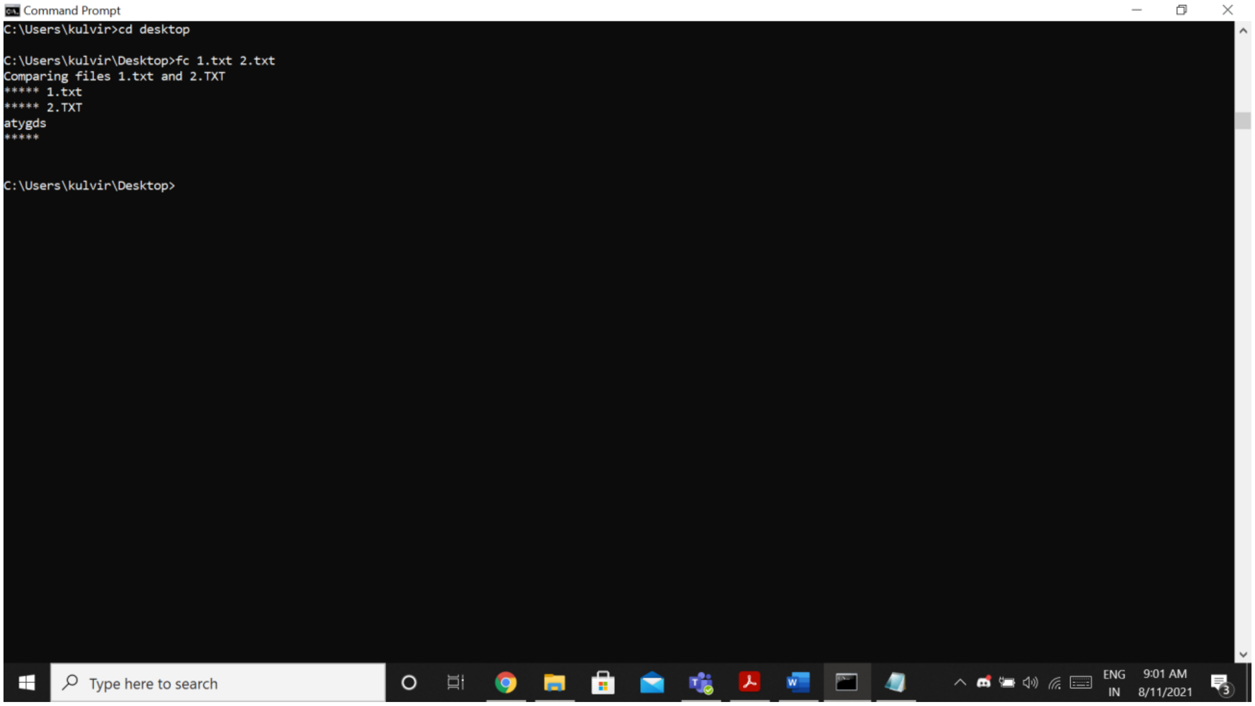
```
C:\Users\kulvir>hostname
KV06

C:\Users\kulvir>pathping google.com

Tracing route to google.com [142.250.195.174]
over a maximum of 30 hops:
  0  KV06.hgu_lan [192.168.1.37]
  1  192.168.1.1
  2  117.203.180.1
  3  static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]
  4  static.ill.218.248.57.170/24.bsnl.in [218.248.57.170]
  5     *        *        *
Computing statistics for 100 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           KV06.hgu_lan [192.168.1.37]
                                0/ 100 =  0%   |
  1   13ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1
                                0/ 100 =  0%   |
  2   16ms     0/ 100 =  0%     0/ 100 =  0%  117.203.180.1
                                0/ 100 =  0%   |
  3   16ms     0/ 100 =  0%     0/ 100 =  0%  static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]
                                0/ 100 =  0%   |
  4   24ms     0/ 100 =  0%     0/ 100 =  0%  static.ill.218.248.57.170/24.bsnl.in [218.248.57.170]

Trace complete.

C:\Users\kulvir>
```

route PRINT



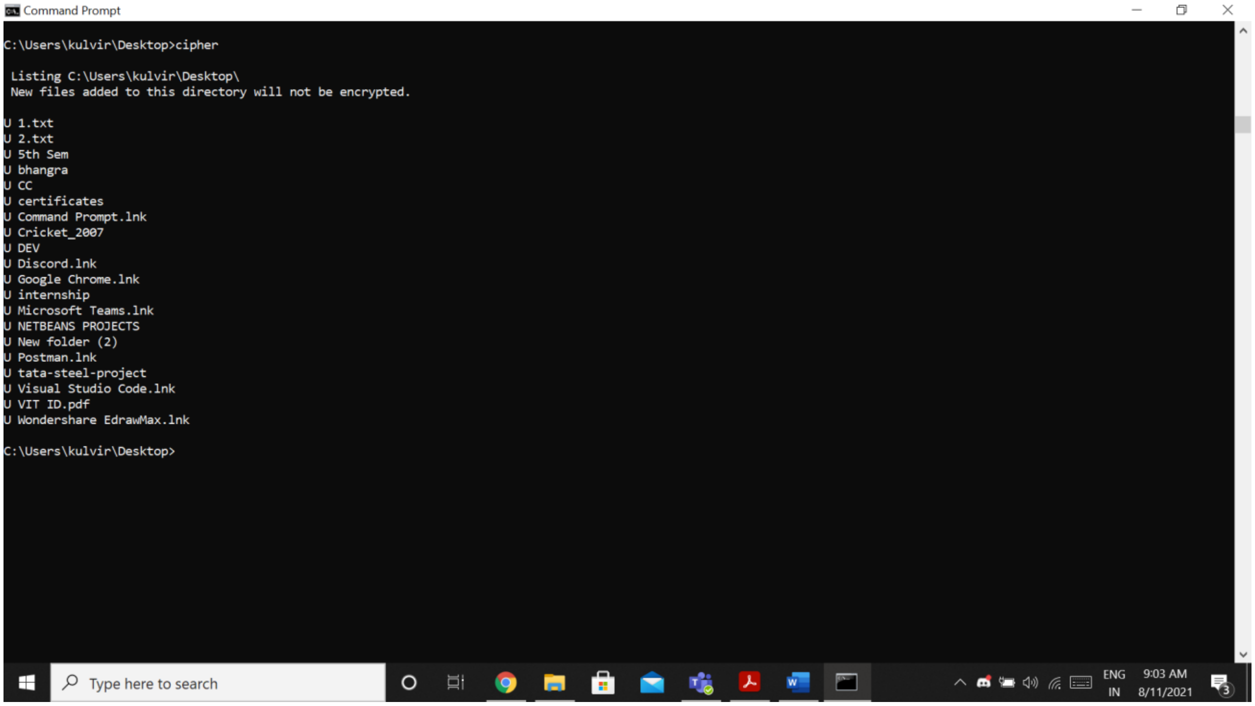
```
C:\Users\kulvir>route PRINT
===========================================================================
Interface List
  4...00 ff 17 d2 72 12 ......TAP-Windows Adapter V9
 16...d2 c5 d3 3f 3f d5 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 18...e2 c5 d3 3f 3f d5 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 24...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  2...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  5...d0 c5 d3 3f 3f d5 ......Qualcomm Atheros QCA9377 Wireless Network Adapter
 11...d0 c5 d3 3f 3f d4 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.37     40
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link      192.168.1.37    296
     192.168.1.37  255.255.255.255         On-link      192.168.1.37    296
    192.168.1.255  255.255.255.255         On-link      192.168.1.37    296
     192.168.80.0    255.255.255.0         On-link      192.168.80.1    291
     192.168.80.1  255.255.255.255         On-link      192.168.80.1    291
   192.168.80.255  255.255.255.255         On-link      192.168.80.1    291
    192.168.159.0    255.255.255.0         On-link     192.168.159.1    291
    192.168.159.1  255.255.255.255         On-link     192.168.159.1    291
  192.168.159.255  255.255.255.255         On-link     192.168.159.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.80.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.159.1    291
        224.0.0.0        240.0.0.0         On-link      192.168.1.37    296
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.80.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.159.1    291
  255.255.255.255  255.255.255.255         On-link      192.168.1.37    296
===========================================================================
Persistent Routes:
  None
```

fc



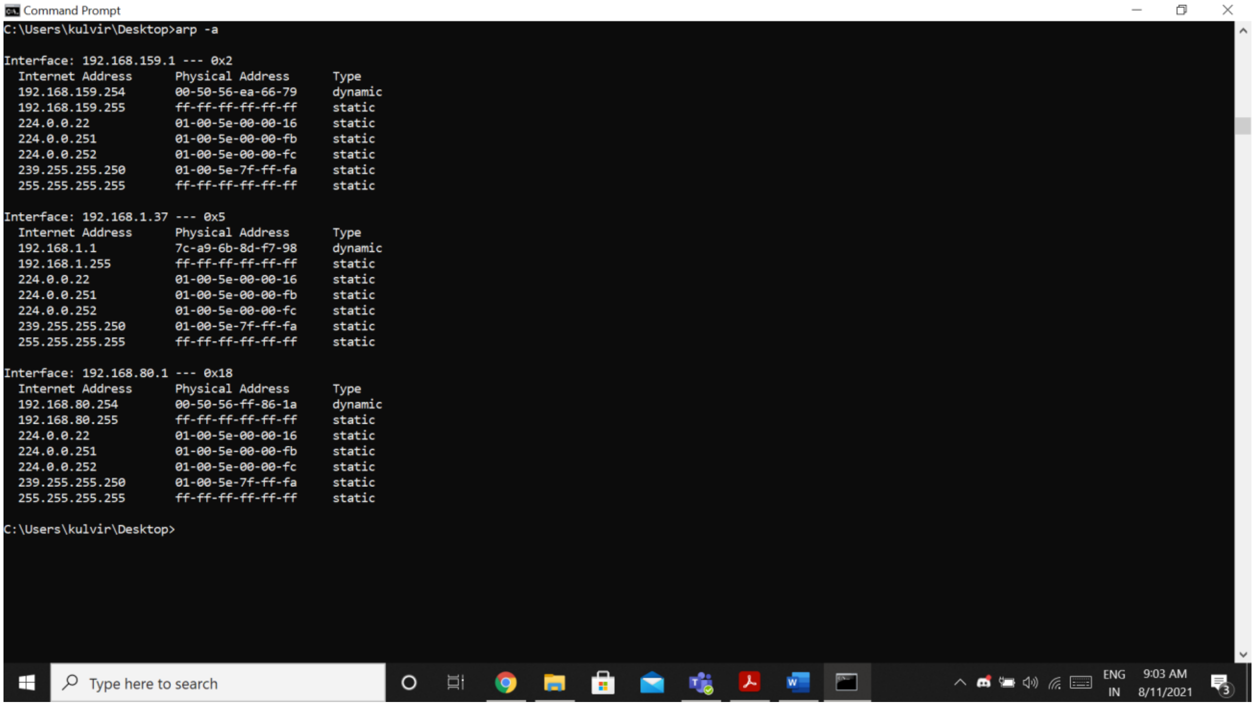
```
C:\Users\kulvir>cd desktop

C:\Users\kulvir\Desktop>fc 1.txt 2.txt
Comparing files 1.txt and 2.TXT
***** 1.txt
***** 2.TXT
atygds
*****


C:\Users\kulvir\Desktop>
```

cipher



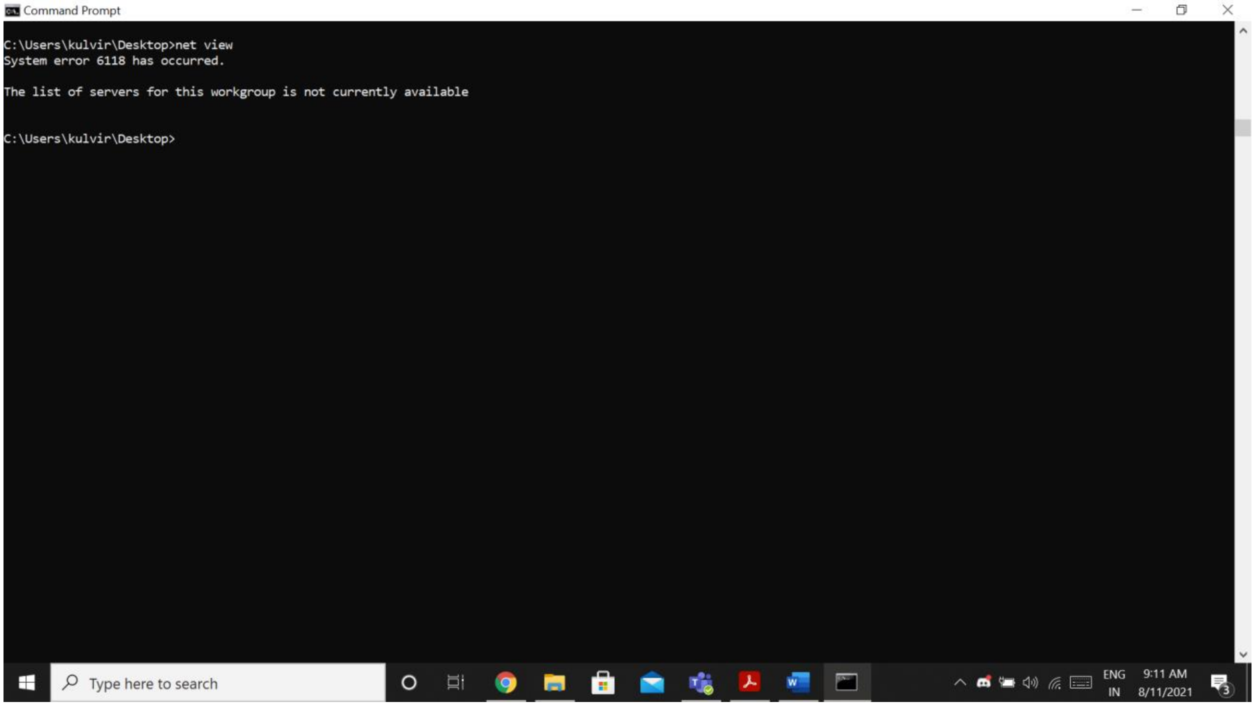
```
C:\Users\kulvir\Desktop>cipher

 Listing C:\Users\kulvir\Desktop\
 New files added to this directory will not be encrypted.

U 1.txt
U 2.txt
U 5th Sem
U bhangra
U CC
U certificates
U Command Prompt.lnk
U Cricket_2007
U DEV
U Discord.lnk
U Google Chrome.lnk
U internship
U Microsoft Teams.lnk
U NETBEANS PROJECTS
U New folder (2)
U Postman.lnk
U tata-steel-project
U Visual Studio Code.lnk
U VIT ID.pdf
U Wondershare EdrawMax.lnk

C:\Users\kulvir\Desktop>
```

arp



```
C:\Users\kulvir\Desktop>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.254       00-50-56-ea-66-79     dynamic
  192.168.159.255       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: 192.168.1.37 --- 0x5
  Internet Address      Physical Address      Type
  192.168.1.1           7c-a9-6b-8d-f7-98     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

Interface: 192.168.80.1 --- 0x18
  Internet Address      Physical Address      Type
  192.168.80.254        00-50-56-ff-86-1a     dynamic
  192.168.80.255        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

C:\Users\kulvir\Desktop>
```

net view



```
C:\Users\kulvir\Desktop>net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available


C:\Users\kulvir\Desktop>
```