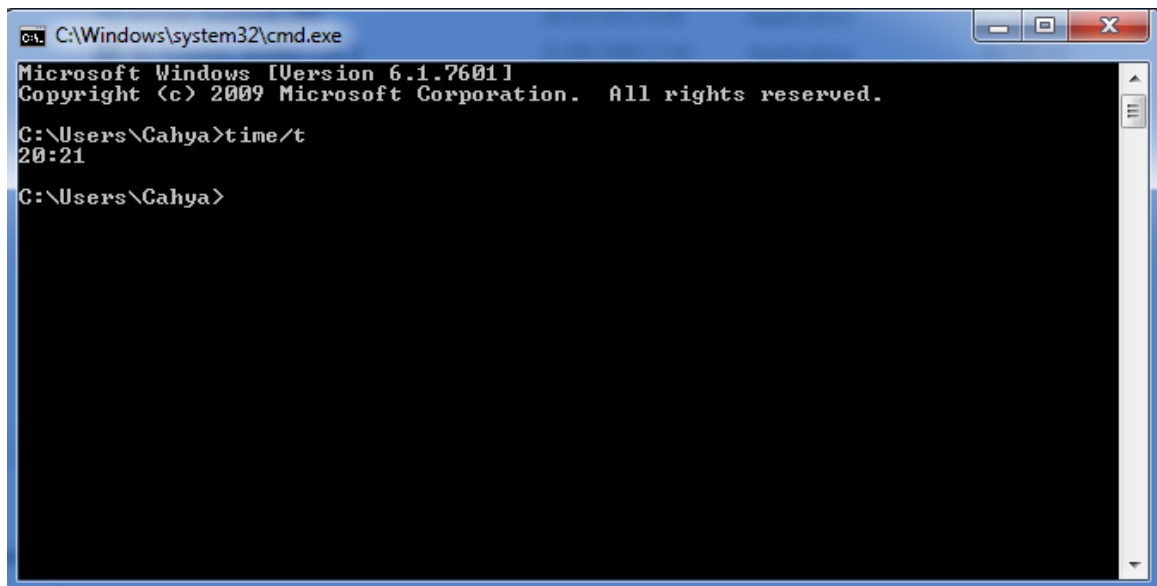


TUGAS WINDOWS FORENSIK

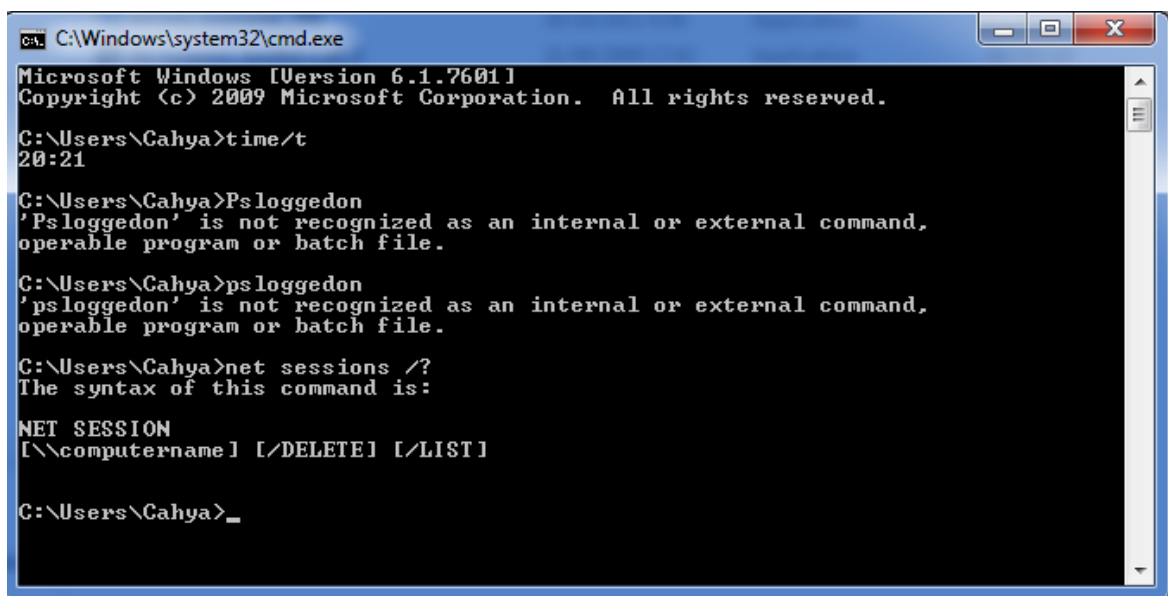


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Cahya>time/t
20:21

C:\Users\Cahya>
```

Perintah time/t diatas berfungsi untuk menunjukkan waktu pada laptop ataupun komputer anda.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Cahya>time/t
20:21

C:\Users\Cahya>Psloggedon
'Psloggedon' is not recognized as an internal or external command,
operable program or batch file.

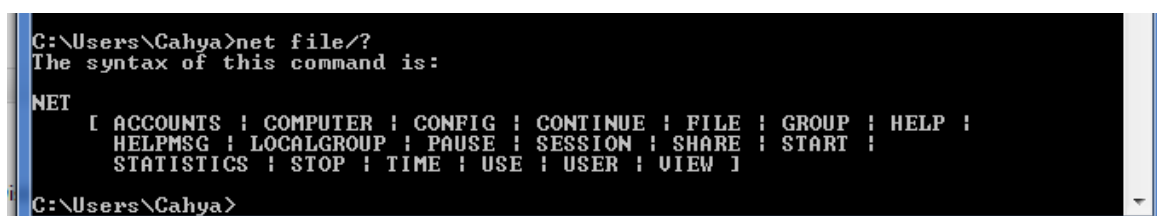
C:\Users\Cahya>psloggedon
'psloggedon' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Cahya>net sessions /?
The syntax of this command is:

NET SESSION
[\\computername] [/DELETE] [/LIST]

C:\Users\Cahya>_
```

Keterangan : perintah net sessions berfungsi untuk menampilkan informasi sesi untuk client dengan nama komputer Boston.



```
C:\Users\Cahya>net file/?
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\Cahya>
```

Keterangan : perintah net file digunakan untuk menutup atau membuang file yang sedang disharing.

```

C:\Users\Cahya>net accounts
Force user logoff how long after time expires?:      Never
Minimum password age <days>:                        0
Maximum password age <days>:                        42
Minimum password length:                             0
Length of password history maintained:               None
Lockout threshold:                                  Never
Lockout duration <minutes>:                          30
Lockout observation window <minutes>:                30
Computer role:                                       WORKSTATION
The command completed successfully.

C:\Users\Cahya>net computer
The syntax of this command is:

NET COMPUTER
\\computername [/ADD : /DEL]

C:\Users\Cahya>net config
The following running services can be controlled:

    Server
    Workstation

The command completed successfully.

C:\Users\Cahya>net group
This command can be used only on a Windows Domain Controller.
More help is available by typing NET HELPMSG 3515.

C:\Users\Cahya>net user
User accounts for \\CAHYA-PC

-----
Administrator          Cahya          Guest
The command completed successfully.

```

Keterangan : perintah net account berfungsi untuk memperbarui basis data akun pengguna dan mengubah persyaratan kata sandi dan untuk logon semua akun.

perintah net config berfungsi untuk menampilkan layanan yang dapat dikonfigurasi yang sedang dijalankan, atau menampilkan dan mengubah pengaturan untuk layanan server atau layanan workstation. Digunakan tanpa parameter.

Sedangkan perintah net user berfungsi untuk menampilkan nama pengguna dari laptop atau komputer yang sedang digunakan.

```

C:\Users\Cahya>net computer
The syntax of this command is:

NET COMPUTER
\\computername [/ADD : /DEL]

C:\Users\Cahya>net config
The following running services can be controlled:

    Server

```

Keterangan : perintah net computer digunakan untuk menambah atau menghapus komputer dari domain database.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>openfiles

INFO: The system global flag 'maintain objects list' needs
to be enabled to see local opened files.
See Openfiles /? for more information.

Files opened remotely via local share points:
-----

INFO: No shared open files found.

C:\Windows\system32>_
```

Untuk menjalankan perintah diatas, kita harus membuka cmd dengan klik kanan run as administrator, kemudian ketikkan perintah diatas “openfiles” , perintah tersebut berfungsi untuk mendiskoneksikan file yang dibuka oleh pengguna jaringan.

```
C:\Users\Cahya>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
                      IP address.
-c (cache)           Lists NBT's cache of remote [machine] names and their IP
addresses
-n (names)           Lists local NetBIOS names.
-r (resolved)        Lists names resolved by broadcast and via WINS
-R (Reload)          Purges and reloads the remote cache name table
-S (Sessions)        Lists sessions table with the destination IP addresses
-s (sessions)        Lists sessions table converting destination IP
                      addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

RemoteName    Remote host machine name.
IP address    Dotted decimal representation of the IP address.
interval      Redisplays selected statistics, pausing interval seconds
              between each display. Press Ctrl+C to stop redisplaying
              statistics.

C:\Users\Cahya>
```

Keterangan : perintah nbtstat sama fungsinya dengan netstat yaitu untuk memantau koneksi jaringan pada suatu komputer, baik itu jaringan lokal maupun jaringan internet

```

C:\Users\Cahya>netstat
Active Connections
    Proto Local Address          Foreign Address         State
C:\Users\Cahya>netstat
Active Connections
    Proto Local Address          Foreign Address         State
C:\Users\Cahya>netstat
Active Connections
    Proto Local Address          Foreign Address         State
    TCP    127.0.0.1:49156         Cahya-PC:49166         ESTABLISHED
    TCP    127.0.0.1:49166         Cahya-PC:49156         ESTABLISHED
    TCP    172.26.31.63:49172     hkg12s09-in-f4:https   TIME_WAIT
    TCP    172.26.31.63:49183     hkg12s13-in-f3:https   TIME_WAIT

```

Keterangan : perintah netstat yaitu berfungsi untuk memantau koneksi jaringan pada suatu komputer, baik itu jaringan lokal maupun jaringan internet

```

C:\Windows\system32\cmd.exe - netstat
There are no entries in the list.

C:\Users\Cahya>openfiles
ERROR: Logged-on user does not have administrative privilege.

C:\Users\Cahya>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
IP address.
-c <cache> Lists NBT's cache of remote [machine] names and their IP
addresses
-n <names> Lists local NetBIOS names.
-r <resolved> Lists names resolved by broadcast and via WINS
-R <Reload> Purges and reloads the remote cache name table
-S <Sessions> Lists sessions table with the destination IP addresses
-s <sessions> Lists sessions table converting destination IP
addresses to computer NETBIOS names.
-RR <ReleaseRefresh> Sends Name Release packets to WINS and then, starts Refr
esh

```

```

C:\Windows\system32\cmd.exe
C:\Users\Cahya>netstat -ano

Active Connections

Proto Local Address Foreign Address State PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 852
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 584
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 420
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 484
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 664
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING 644
TCP 0.0.0.0:49158 0.0.0.0:0 LISTENING 2532
TCP 127.0.0.1:1001 0.0.0.0:0 LISTENING 4
TCP 127.0.0.1:49156 0.0.0.0:0 LISTENING 1916
TCP 127.0.0.1:49156 127.0.0.1:49166 ESTABLISHED 1916
TCP 127.0.0.1:49166 127.0.0.1:49156 ESTABLISHED 3592
TCP 172.26.31.63:139 0.0.0.0:0 LISTENING 4
TCP 172.26.31.63:49172 216.58.203.4:443 TIME_WAIT 0
TCP 172.26.31.63:49183 172.217.24.195:443 TIME_WAIT 0
TCP 172.26.31.63:49190 10.20.173.44:8080 TIME_WAIT 0
TCP 172.26.31.63:49191 10.20.173.44:8080 TIME_WAIT 0
TCP 172.26.31.63:49192 192.168.185.20:8080 TIME_WAIT 0
TCP 172.26.31.63:49194 10.10.100.5:80 TIME_WAIT 0
TCP 172.26.31.63:49195 10.10.100.5:80 TIME_WAIT 0
TCP 172.26.31.63:49196 10.10.100.5:80 TIME_WAIT 0
TCP 172.26.31.63:49197 10.10.100.5:80 TIME_WAIT 0
TCP 172.26.31.63:49198 10.10.100.5:80 TIME_WAIT 0
TCP 172.26.31.63:49199 172.26.31.1:80 TIME_WAIT 0
TCP 172.26.31.63:49200 172.26.31.1:80 TIME_WAIT 0
TCP 172.26.31.63:49201 172.26.31.1:80 TIME_WAIT 0
TCP 172.26.31.63:49202 172.26.31.1:80 TIME_WAIT 0

```

Keterangan : perintah netstat -ano berfungsi untuk menampilkan semua koneksi baik yang listening maupun yang tidak, dan menampilkan alamat port dalam bentuk numerik serta menampilkan PID (Process ID) untuk setiap koneksi.

```

C:\Windows\system32\cmd.exe - netstat
There are no entries in the list.

C:\Users\Cahya>openfiles
ERROR: Logged-on user does not have administrative privilege.

C:\Users\Cahya>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
                    IP address.
-c <cache>          Lists NBT's cache of remote [machine] names and their IP
addresses
-n <names>          Lists local NetBIOS names.
-r <resolved>       Lists names resolved by broadcast and via WINS
-R <Reload>         Purges and reloads the remote cache name table
-S <Sessions>       Lists sessions table with the destination IP addresses
-s <sessions>       Lists sessions table converting destination IP
                    addresses to computer NETBIOS names.
-RR <ReleaseRefresh> Sends Name Release packets to WINS and then, starts Refr
esh

C:\Windows\system32\cmd.exe

Proto Local Address          Foreign Address         State

C:\Users\Cahya>netstat -r
=====
Interface List
13...66 6d 57 3e 02 bd .....Microsoft Virtual WiFi Miniport Adapter
12...44 6d 57 3e 02 bd .....Atheros AR9002WB-1NG Wireless Network Adapter
11...04 7d 7b ab 6c 71 .....Atheros AR8152/8158 PCI-E Fast Ethernet Controller
(NDIS 6.20)
1.....Software Loopback Interface 1
14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
15...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          172.26.31.1      172.26.31.63     25
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
172.26.31.0                255.255.255.0    On-link          172.26.31.63     281
172.26.31.63               255.255.255.255  On-link          172.26.31.63     281
172.26.31.255              255.255.255.255  On-link          172.26.31.63     281
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          172.26.31.63     281
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          172.26.31.63     281
=====
Persistent Routes:

```

Keterangan : perintah netstat -r berfungsi untuk menampilkan routing table

```

C:\Windows\system32\cmd.exe - netstat
There are no entries in the list.

C:\Users\Cahya>openfiles
ERROR: Logged-on user does not have administrative privilege.

C:\Users\Cahya>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
                    IP address.
-c <cache>          Lists NBT's cache of remote [machine] names and their IP
addresses
-n <names>          Lists local NetBIOS names.
-r <resolved>       Lists names resolved by broadcast and via WINS
-R <Reload>         Purges and reloads the remote cache name table
-S <Sessions>       Lists sessions table with the destination IP addresses
-s <sessions>       Lists sessions table converting destination IP
                    addresses to computer NETBIOS names.
-RR <ReleaseRefresh> Sends Name Release packets to WINS and then, starts Refr
esh

```

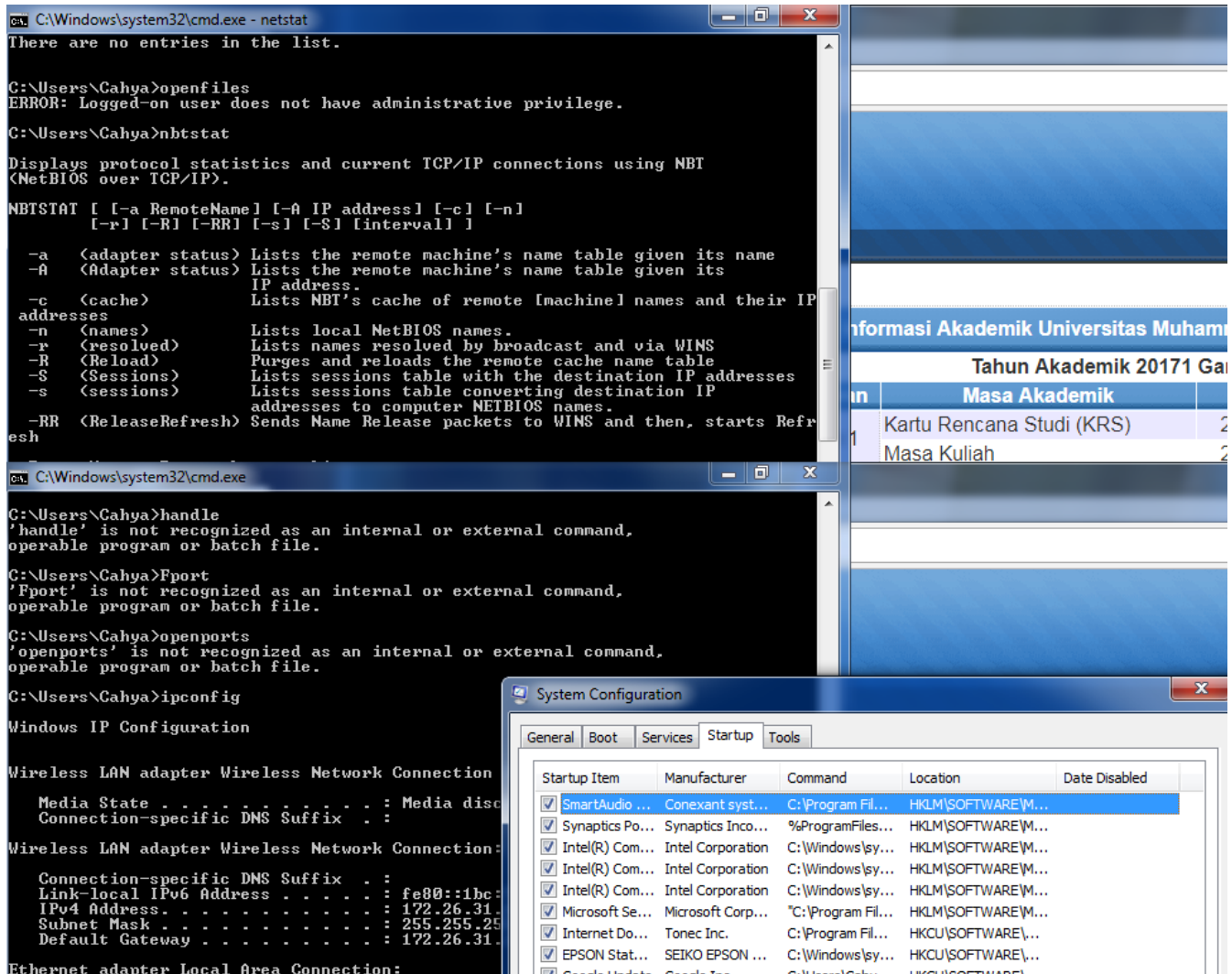
```

C:\Windows\system32\cmd.exe
C:\Users\Cahya>Tasklist

Image Name                PID Session Name        Session#    Mem Usage
=====
System Idle Process        0 Services            0           24 K
System                    4 Services            0          956 K
smss.exe                  348 Services            0           796 K
csrss.exe                  488 Services            0          3.636 K
wininit.exe                584 Services            0          3.544 K
csrss.exe                  612 Console            1          36.416 K
services.exe               644 Services            0           7.076 K
lsass.exe                  664 Services            0           8.096 K
lsm.exe                    672 Services            0          3.580 K
svchost.exe                776 Services            0           8.152 K
svchost.exe                852 Services            0           8.180 K
MsMpEng.exe                912 Services            0          81.892 K
winlogon.exe               964 Console            1           5.228 K
svchost.exe                420 Services            0          15.216 K
svchost.exe                448 Services            0          79.892 K
svchost.exe                536 Services            0          12.248 K
svchost.exe                484 Services            0          28.580 K
svchost.exe               1164 Services            0          13.600 K
wlanext.exe               1272 Services            0           4.820 K
conhost.exe               1280 Services            0           2.284 K
spoolsv.exe               1376 Services            0           9.484 K
svchost.exe               1404 Services            0          10.536 K
svchost.exe               1504 Services            0           5.436 K
escsvc64.exe              1564 Services            0           4.952 K
NitroPDFDriverService10x6 1616 Services            0           2.432 K
Nitro_UpdateService.exe   1656 Services            0           4.348 K
PsiService_2.exe          1736 Services            0           2.936 K
taskhost.exe              1808 Console            1          14.204 K

```

Keterangan : perintah tasklist berfungsi untuk menampilkan daftar task yang sedang berjalan pada PC anda. Perintah tasklist ini bisa menemukan task yang tersembunyi dari task manager.



Keterangan : perintah ipconfig ini berfungsi untuk menampilkan semua alamat sistem Networks dari komputer, atau bisa dikatakan untuk melihat informasi jaringan atau informasi IP yang terpasang di Networks adapter.