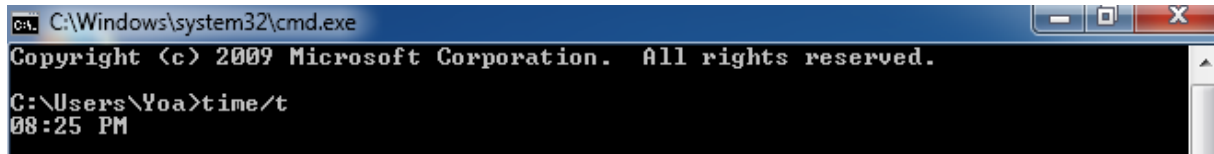


Nama : Anik Nur Novitasari Eka Septianingrum
NIM : 1710652004
Class : TI- Sore

TUGAS WINDOWS FORENSIK

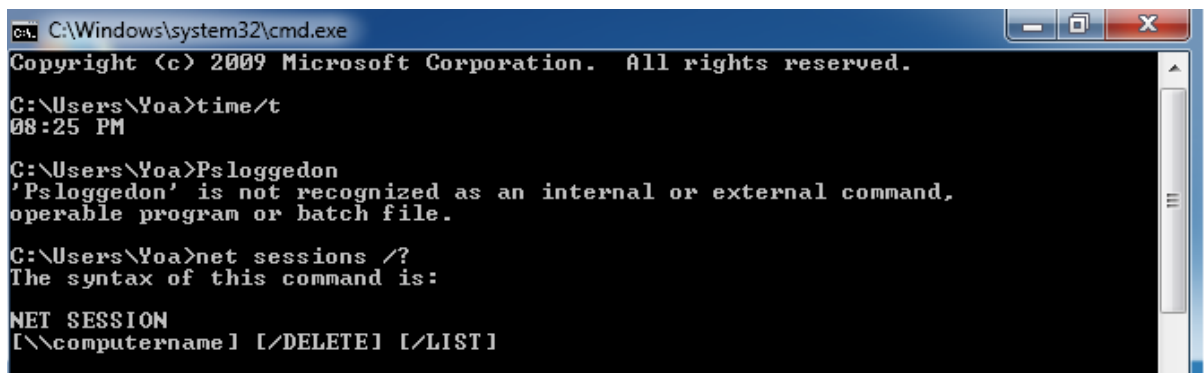
1. Time



```
C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Yoa>time/t
08:25 PM
```

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

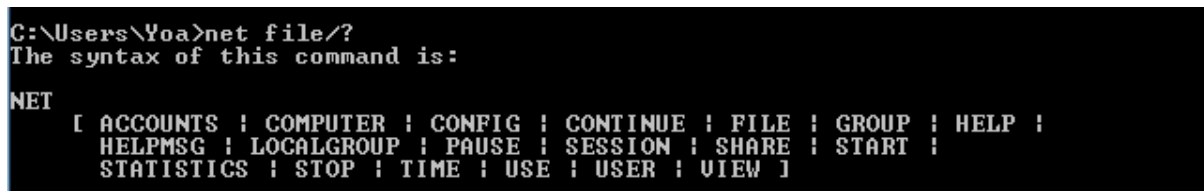
2. Net Sessions



```
C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Yoa>time/t
08:25 PM
C:\Users\Yoa>Psloggedon
'Psloggedon' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Yoa>net sessions /?
The syntax of this command is:
NET SESSION
[\\computername] [/DELETE] [/LIST]
```

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

3. Net File



```
C:\Users\Yoa>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 ]
```

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

4. Net Accounts

```

C:\Users\Yoa>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.

```

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

5. Net Config dan Net User

```

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

    Server
    Workstation

The command completed successfully.

```

Keterangan: 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.

```

C:\Users\Yoa>net user

User accounts for \\YOA-PC

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

C:\Users\Yoa>

```

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

6. Net Computer

```

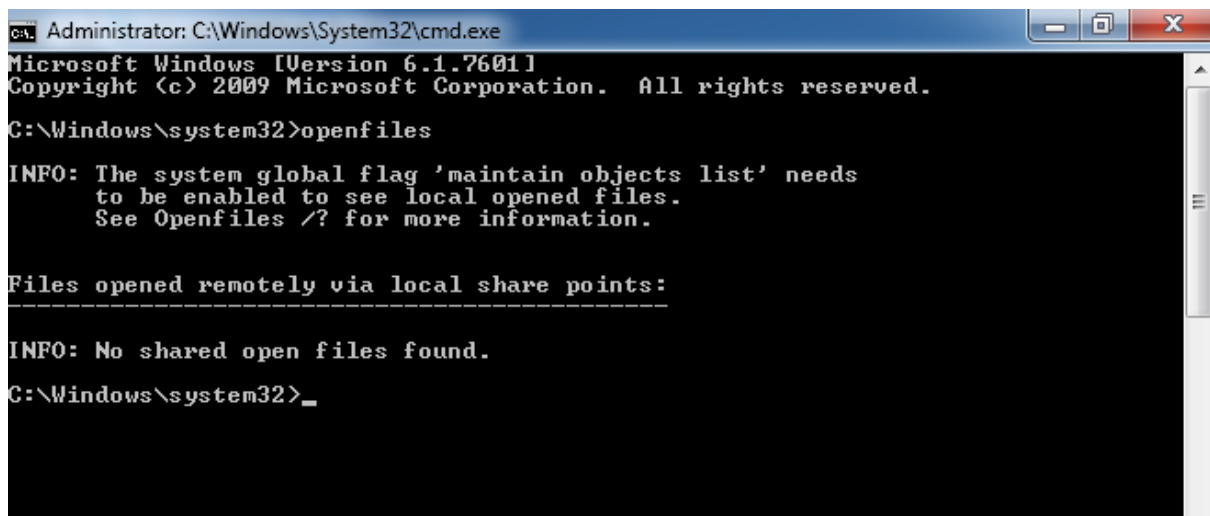
C:\Users\Yoa>net computer
The syntax of this command is:

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

```

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

7. Openfiles



```
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.

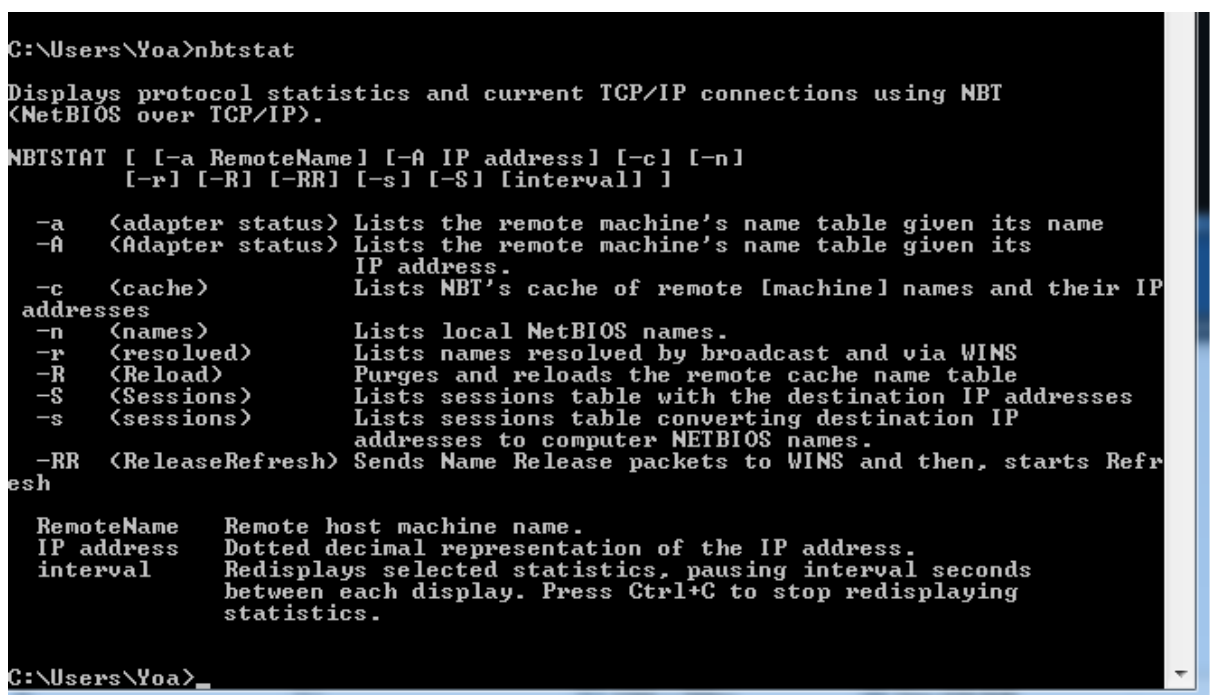
Files opened remotely via local share points:
-----

INFO: No shared open files found.

C:\Windows\system32>_
```

Open File digunakan 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.

8. NBStat



```
C:\Users\Yoa>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] ]

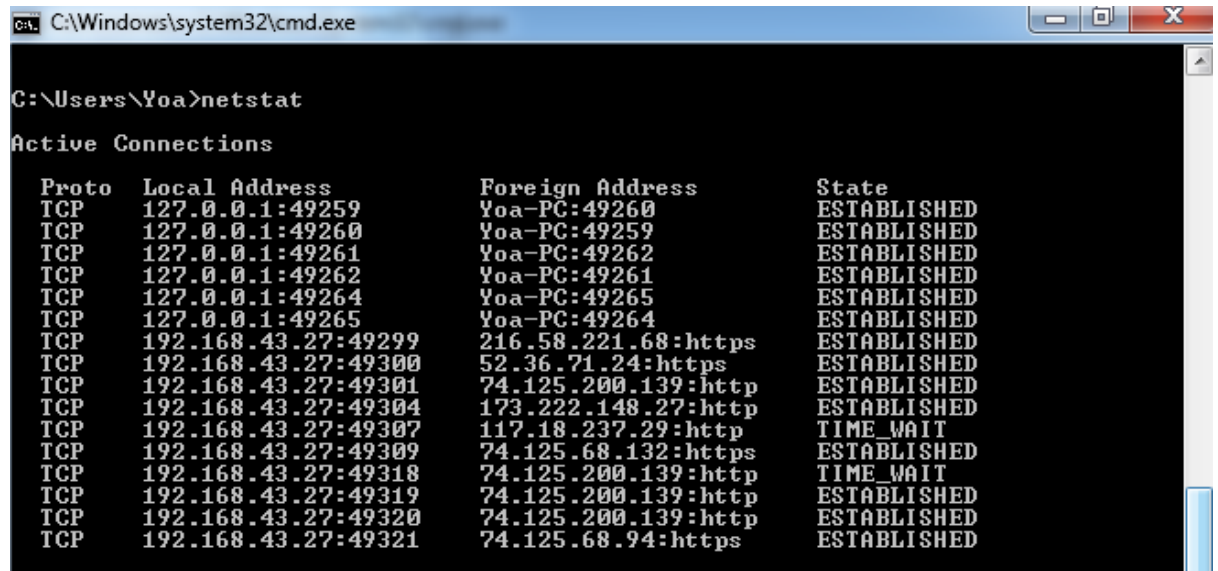
-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
                      IP address.
-c <cache>           Lists NBT's cache of remote [machine] names and their IP
addresses
-n <names>           Lists local NetBIOS 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\Yoa>_
```

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

9. Net Stat



```
C:\Windows\system32\cmd.exe

C:\Users\Yoa>netstat

Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:49259          Yoa-PC:49260           ESTABLISHED
TCP   127.0.0.1:49260          Yoa-PC:49259           ESTABLISHED
TCP   127.0.0.1:49261          Yoa-PC:49262           ESTABLISHED
TCP   127.0.0.1:49262          Yoa-PC:49261           ESTABLISHED
TCP   127.0.0.1:49264          Yoa-PC:49265           ESTABLISHED
TCP   127.0.0.1:49265          Yoa-PC:49264           ESTABLISHED
TCP   192.168.43.27:49299      216.58.221.68:https     ESTABLISHED
TCP   192.168.43.27:49300      52.36.71.24:https       ESTABLISHED
TCP   192.168.43.27:49301      74.125.200.139:http     ESTABLISHED
TCP   192.168.43.27:49304      173.222.148.27:http    ESTABLISHED
TCP   192.168.43.27:49307      117.18.237.29:http     TIME_WAIT
TCP   192.168.43.27:49309      74.125.68.132:https     ESTABLISHED
TCP   192.168.43.27:49318      74.125.200.139:http    TIME_WAIT
TCP   192.168.43.27:49319      74.125.200.139:http     ESTABLISHED
TCP   192.168.43.27:49320      74.125.200.139:http     ESTABLISHED
TCP   192.168.43.27:49321      74.125.68.94:https      ESTABLISHED
```

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

10. Netstat -ano

```

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

Active Connections

Proto Local Address          Foreign Address         State       PID
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING   916
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  520
TCP   0.0.0.0:49153           0.0.0.0:0               LISTENING 1016
TCP   0.0.0.0:49154           0.0.0.0:0               LISTENING  320
TCP   0.0.0.0:49156           0.0.0.0:0               LISTENING  648
TCP   0.0.0.0:49157           0.0.0.0:0               LISTENING  584
TCP   0.0.0.0:49158           0.0.0.0:0               LISTENING 2596
TCP   127.0.0.1:1001          0.0.0.0:0               LISTENING    4
TCP   127.0.0.1:49155         0.0.0.0:0               LISTENING  1440
TCP   127.0.0.1:49259         127.0.0.1:49260         ESTABLISHED 912
TCP   127.0.0.1:49260         127.0.0.1:49259         ESTABLISHED 912
TCP   127.0.0.1:49261         127.0.0.1:49262         ESTABLISHED 4048
TCP   127.0.0.1:49262         127.0.0.1:49261         ESTABLISHED 4048
TCP   127.0.0.1:49264         127.0.0.1:49265         ESTABLISHED 3324
TCP   127.0.0.1:49265         127.0.0.1:49264         ESTABLISHED 3324
TCP   192.168.43.27:139       0.0.0.0:0               LISTENING    4
TCP   192.168.43.27:49299    216.58.221.68:443       ESTABLISHED 912
TCP   192.168.43.27:49304    173.222.148.27:80       ESTABLISHED 912
TCP   192.168.43.27:49309    74.125.68.132:443       TIME_WAIT    0
TCP   192.168.43.27:49322    52.26.69.182:443        TIME_WAIT    0
TCP   192.168.43.27:49326    52.84.225.12:443        ESTABLISHED 912
TCP   192.168.43.27:49327    52.84.223.173:443       ESTABLISHED 912
TCP   192.168.43.27:49330    173.222.148.27:80       TIME_WAIT    0
TCP   192.168.43.27:49331    52.172.193.7:443        ESTABLISHED 1628
TCP   192.168.43.27:49334    13.107.3.128:443        ESTABLISHED 2612
TCP   192.168.43.27:49337    114.125.83.155:80       ESTABLISHED 1628
TCP   192.168.43.27:49338    23.102.4.253:443        ESTABLISHED 2612
TCP   192.168.43.27:49339    118.98.93.8:80          ESTABLISHED 1628
TCP   192.168.43.27:49342    23.102.4.253:443        ESTABLISHED 1064
TCP   192.168.43.27:49344    114.125.83.155:80       ESTABLISHED 1064
TCP   192.168.43.27:49346    168.63.18.79:443        ESTABLISHED 2612
TCP   [::]:135               [::]:0                  LISTENING   916
TCP   [::]:445               [::]:0                  LISTENING    4
TCP   [::]:49152             [::]:0                  LISTENING  520
TCP   [::]:49153             [::]:0                  LISTENING 1016
TCP   [::]:49154             [::]:0                  LISTENING  320
TCP   [::]:49156             [::]:0                  LISTENING  648
TCP   [::]:49157             [::]:0                  LISTENING  584
TCP   [::]:49158             [::]:0                  LISTENING 2596
UDP   0.0.0.0:500            ***                     320
UDP   0.0.0.0:4500           ***                     320
UDP   0.0.0.0:5355           ***                     1180
UDP   192.168.43.27:137      ***                     4
UDP   192.168.43.27:138      ***                     4
UDP   [::]:500               ***                     320
UDP   [::]:4500              ***                     320
UDP   [::]:5355              ***                     1180

C:\Users\Yoa>_

```

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

11. Netstat -r

```
C:\Users\Yoa>netstat -r
=====
Interface List
11...34 e6 ad 93 da 9b .....Intel(R) Dual Band Wireless-AC 3160
1.....Software Loopback Interface 1
20...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface          Metric
0.0.0.0                    0.0.0.0          192.168.43.1        192.168.43.27      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
192.168.43.0                255.255.255.0    On-link             192.168.43.27      281
192.168.43.27              255.255.255.255  On-link             192.168.43.27      281
192.168.43.255             255.255.255.255  On-link             192.168.43.27      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             192.168.43.27      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             192.168.43.27      281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
12      58 ::/0 On-link
1       306 ::1/128 On-link
12      58 2001::/32 On-link
12      306 2001:0:ca03:dbd3:20ec:30c8:3f57:d4e4/128 On-link
11      281 fe80::/64 On-link
12      306 fe80::/64 On-link
12      306 fe80::20ec:30c8:3f57:d4e4/128 On-link
11      281 fe80::c105:64ee:28be:24c6/128 On-link
1       306 ff00::/8 On-link
12      306 ff00::/8 On-link
11      281 ff00::/8 On-link
=====
Persistent Routes:
None

C:\Users\Yoa>
```

Keterangan : Perintah netstat -r berfungsi untuk menampilkan routing table

12. TaskList

C:\Windows\system32\cmd.exe

C:\Users\Yoa>Tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,116 K
smss.exe	272	Services	0	1,172 K
csrss.exe	416	Services	0	4,596 K
wininit.exe	520	Services	0	4,828 K
csrss.exe	544	Console	1	38,552 K
services.exe	584	Services	0	9,596 K
winlogon.exe	620	Console	1	7,772 K
lsass.exe	648	Services	0	11,684 K
lsm.exe	656	Services	0	4,448 K
svchost.exe	784	Services	0	10,324 K
nvsvc.exe	848	Services	0	8,188 K
nvSCPAPISrvr.exe	872	Services	0	6,044 K
svchost.exe	916	Services	0	9,084 K
svchost.exe	1016	Services	0	18,172 K
svchost.exe	296	Services	0	112,236 K
svchost.exe	320	Services	0	37,060 K
svchost.exe	1032	Services	0	13,120 K
igfxCUIService.exe	1088	Services	0	7,368 K
svchost.exe	1180	Services	0	37,144 K
nvxdsync.exe	1264	Console	1	22,584 K
nvsvc.exe	1272	Console	1	14,912 K
dwm.exe	1388	Console	1	29,844 K
explorer.exe	1440	Console	1	81,904 K
spoolsv.exe	1504	Services	0	12,372 K
svchost.exe	1532	Services	0	12,748 K
OfficeClickToRun.exe	1628	Services	0	53,660 K
taskhost.exe	1840	Console	1	9,112 K
taskeng.exe	1892	Console	1	7,160 K
ggdllhost.exe	1944	Console	1	2,076 K
svchost.exe	2004	Services	0	9,312 K
PresentationFontCache.exe	2308	Services	0	17,036 K
RAUCpl64.exe	2440	Console	1	11,224 K
ONENOTEM.EXE	2528	Console	1	1,480 K
igfxEM.exe	2512	Console	1	10,988 K
svchost.exe	2596	Services	0	5,728 K
SearchIndexer.exe	2700	Services	0	18,560 K
igfxHK.exe	812	Console	1	8,916 K
igfxTray.exe	2404	Console	1	9,372 K
ggdllhost.exe	3192	Console	1	8,376 K
svchost.exe	3964	Services	0	41,388 K
svchost.exe	3992	Services	0	21,972 K
cmd.exe	3364	Console	1	3,728 K
conhost.exe	1000	Console	1	5,844 K
mspaint.exe	3544	Console	1	70,456 K
cmd.exe	2780	Console	1	3,604 K
conhost.exe	3584	Console	1	5,724 K
firefox.exe	912	Console	1	251,856 K
firefox.exe	4048	Console	1	122,780 K
firefox.exe	3324	Console	1	62,016 K
taskeng.exe	3836	Services	0	5,440 K
sppsvc.exe	3316	Services	0	8,548 K
OfficeClickToRun.exe	2612	Console	1	24,412 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.

13. IPConfig

```
C:\Users\Yoa>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c105:64ee:28be:24c6%11
    IPv4 Address. . . . . : 192.168.43.27
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.43.1

Tunnel adapter isatap.{01937880-186A-4AC8-A933-47DE9ABC7FEF}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:ca03:dbd3:20ec:30c8:3f57:d4e4
    Link-local IPv6 Address . . . . . : fe80::20ec:30c8:3f57:d4e4%12
    Default Gateway . . . . . : ::

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

C:\Users\Yoa>
```

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.