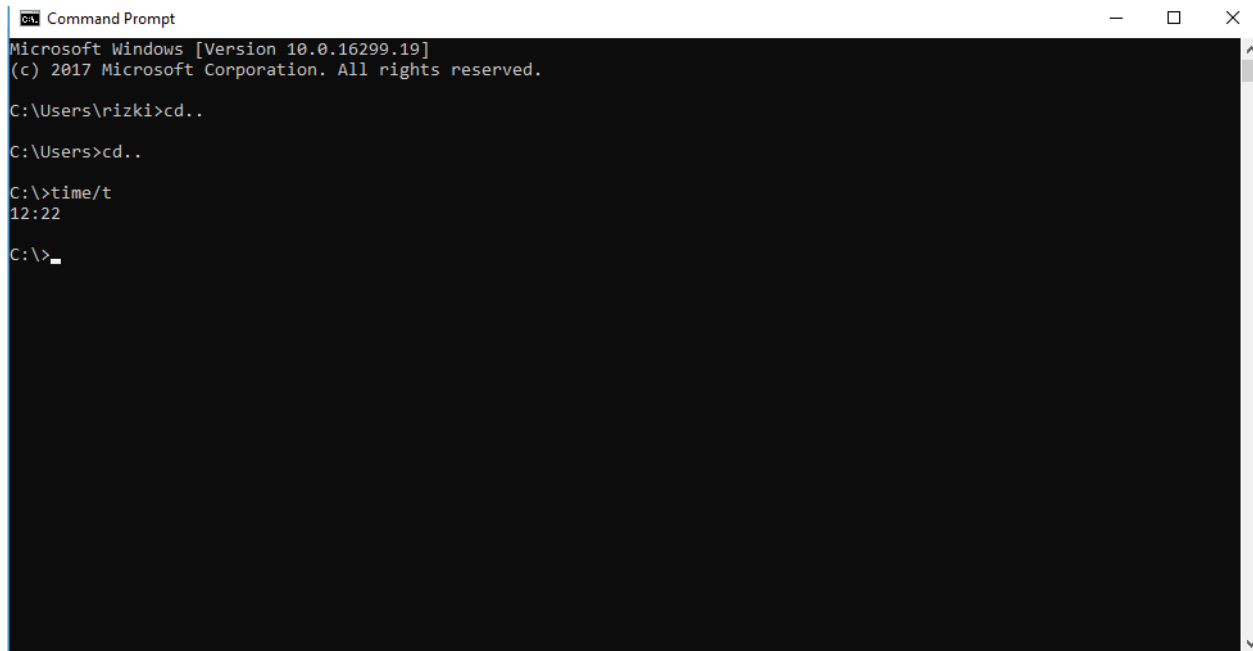


**Nama** : M. Fatkhur Rohman  
**Nim** : 1410652017  
**Matkul** : Forensik Digital

## 1. Time

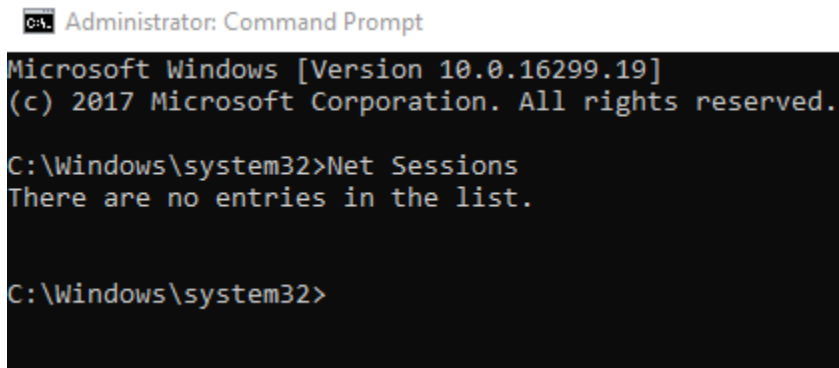


```
Command Prompt
Microsoft Windows [Version 10.0.16299.19]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\rizki>cd..
C:\Users>cd..
C:\>time/t
12:22
C:\>_
```

Kegunaan : Menampilkan garis waktu yang akurat tentang kejadian yang telah terjadi pada system

## 2. Net Sessions



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.16299.19]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>Net Sessions
There are no entries in the list.

C:\Windows\system32>
```

Kegunaan : Mengumpulkan informasi tentang pengguna yang login ke system, baik local maupun local dari jarak jauh

```
Administrator: Command Prompt

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

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

C:\>
```

Kegunaan : Memberikan informasi tentang username dan ip yang digunakan untuk mengakses system via remote login session dan tipe system client yang diakses

### 3. Net File

```
Administrator: Command Prompt

INFO: No shared open files found.

C:\>Net File/?
The syntax of this command is:

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

C:\>
```

Kegunaan : menampilkan nama semua file bersama yang terbuka pada sebuah system

#### 4. Openfiles

```
Administrator: Command Prompt
INFO: No shared open files found.

C:\>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:\>
```

Kegunaan : menampilkan daftar file yang sudah ditutup dan folder yang dibuka pada system

#### 5. Netstat -ano

```
Administrator: Command Prompt
INFO: No shared open files found.

C:\>netstat -ano

Active Connections

  Proto Local Address           Foreign Address         State       PID
  ---
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING   8
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING   4
  TCP    0.0.0.0:49664            0.0.0.0:0               LISTENING   636
  TCP    0.0.0.0:49665            0.0.0.0:0               LISTENING   1172
  TCP    0.0.0.0:49666            0.0.0.0:0               LISTENING   1524
  TCP    0.0.0.0:49667            0.0.0.0:0               LISTENING   2520
  TCP    0.0.0.0:49668            0.0.0.0:0               LISTENING   788
  TCP    0.0.0.0:49669            0.0.0.0:0               LISTENING   780
  TCP    127.0.0.1:1001           0.0.0.0:0               LISTENING   4
  TCP    127.0.0.1:50604         0.0.0.0:0               LISTENING   7892
  TCP    [::]:135                [::]:0                  LISTENING   8
  TCP    [::]:445                [::]:0                  LISTENING   4
  TCP    [::]:49664              [::]:0                  LISTENING   636
  TCP    [::]:49665              [::]:0                  LISTENING   1172
  TCP    [::]:49666              [::]:0                  LISTENING   1524
  TCP    [::]:49667              [::]:0                  LISTENING   2520
  TCP    [::]:49668              [::]:0                  LISTENING   788
  TCP    [::]:49669              [::]:0                  LISTENING   780
  UDP    0.0.0.0:5050            *:0                      LISTENING   6000
  UDP    127.0.0.1:1900          *:0                      LISTENING   4076
  UDP    127.0.0.1:49664         *:0                      LISTENING   2736
  UDP    127.0.0.1:53169        *:0                      LISTENING   4076
  UDP    [::1]:1900              *:0                      LISTENING   4076
```

Kegunaan : menampilkan koneksi jaringan tcp dan udp

## 6. Netstat -r

```
C:\> netstat -r
```

```
=====
```

```
Interface List
```

```
9...12 d9 62 e8 e2 8b .....Microsoft Wi-Fi Direct Virtual Adapter
```

```
3...c0 d9 62 e8 e2 8b .....Qualcomm Atheros AR956x Wireless Network Adapter
```

```
1.....Software Loopback Interface 1
```

```
2...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
```

```
=====
```

```
IPv4 Route Table
```

```
=====
```

```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface	Metric
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
224.0.0.0	240.0.0.0		On-link	127.0.0.1	331
255.255.255.255	255.255.255.255		On-link	127.0.0.1	331

```
=====
```

```
Persistent Routes:
```

```
None
```

```
IPv6 Route Table
```

```
=====
```

```
Active Routes:
```

If	Metric	Network	Destination	Gateway
1	331	::1/128		On-link

Kegunaan : menampilkan table routing dan menunjukkan rute yang terus menerus diaktifkan pada system

## 7. Tasklist

```
Administrator: Command Prompt

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

C:\>Tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	52 K
smss.exe	384	Services	0	480 K
csrss.exe	548	Services	0	1.816 K
wininit.exe	636	Services	0	2.904 K
services.exe	780	Services	0	5.948 K
lsass.exe	788	Services	0	7.676 K
svchost.exe	920	Services	0	384 K
fontdrvhost.exe	944	Services	0	404 K
svchost.exe	964	Services	0	16.504 K
svchost.exe	8	Services	0	11.872 K
svchost.exe	576	Services	0	4.524 K
svchost.exe	1172	Services	0	8.152 K
svchost.exe	1208	Services	0	4.332 K
svchost.exe	1216	Services	0	5.244 K
svchost.exe	1336	Services	0	2.072 K
svchost.exe	1348	Services	0	5.216 K
svchost.exe	1408	Services	0	42.520 K
svchost.exe	1416	Services	0	1.436 K
Memory Compression	1456	Services	0	41.104 K
svchost.exe	1524	Services	0	10.348 K

Kegunaan : memberikan daftar saat ini dari semua tugas yang berjalan pada pc

## 8. Tasklist /v

Administrator: Command Prompt

```
C:\>Tasklist /v
```

Image Name	PID	Session Name CPU Time Window Title	Session#	Mem Usage	Status	User Name
System Idle Process	0	Services	0	8 K	Unknown	NT AUTHORITY\SYSTEM
System	4	Services	0	52 K	Unknown	N/A
smss.exe	0:38:27	N/A	0	480 K	Unknown	NT AUTHORITY\SYSTEM
csrss.exe	384	Services	0	1.820 K	Unknown	NT AUTHORITY\SYSTEM
wininit.exe	0:00:00	N/A	0	2.904 K	Unknown	NT AUTHORITY\SYSTEM
services.exe	548	Services	0	5.952 K	Unknown	NT AUTHORITY\SYSTEM
lsass.exe	0:00:01	N/A	0	7.828 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	780	Services	0	384 K	Unknown	NT AUTHORITY\SYSTEM
fontdrvhost.exe	0:00:13	N/A	0	404 K	Unknown	Font Driver Host\UMFD-0
svchost.exe	920	Services	0	16.492 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	944	Services	0	11.840 K	Unknown	NT AUTHORITY\NETWORK SERVICE
svchost.exe	8	Services	0	4.528 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	0:01:07	N/A	0			
svchost.exe	576	Services	0			
	0:00:00	N/A				

Kegunaan : menyediakan informasi tentang daftar yang di olah termasuk nama, PID dan jumlah sesi untuk proses tersebut

## 9. Netstat -o

Select Administrator: Command Prompt

```
C:\>netstat -o
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
-------	---------------	-----------------	-------	-----

```
C:\>
```

Kegunaan : menampilkan proses id dari proses yang bertanggung jawab atas koneksi jaringan