

TUGAS KELAS DIGITAL FORENSIC
WINDOWS FORENSIC



Octa Yusak Puraja

Kelas Sore-1510652006

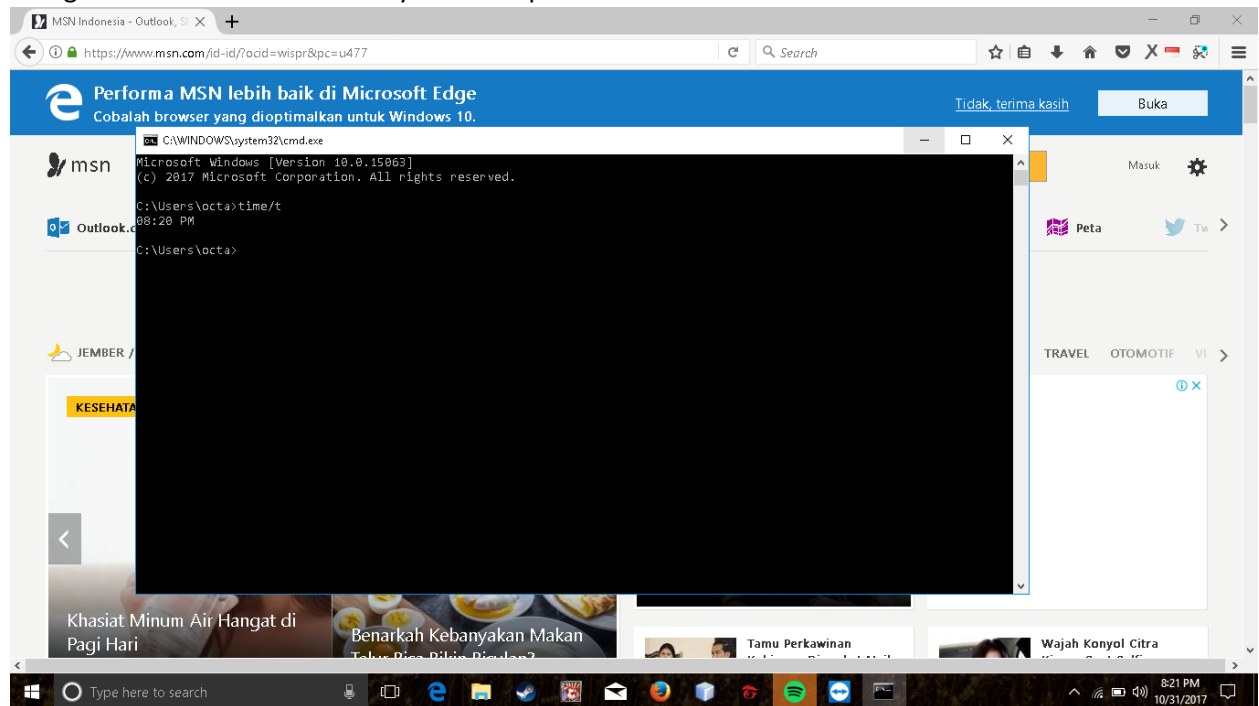
UNIVERSITAS MUHAMMADIYAH

JEMBER

2017

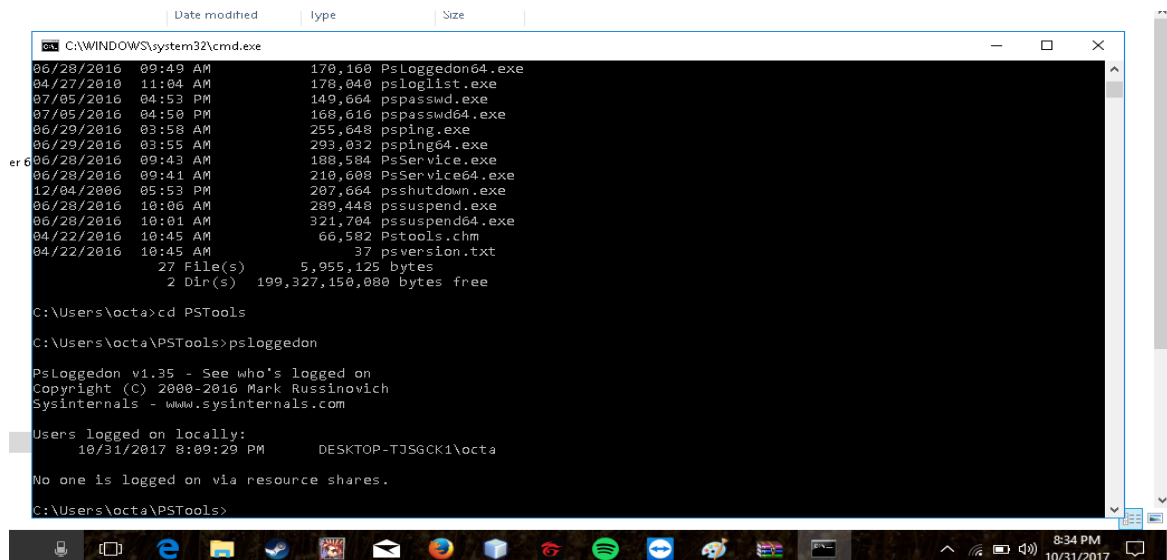
1. SYSTEM TIME

Perintah yang digunakan pada *command prompt* yaitu **time/t**. Perintah ini digunakan untuk mengetahui waktu dari sebuah system computer.



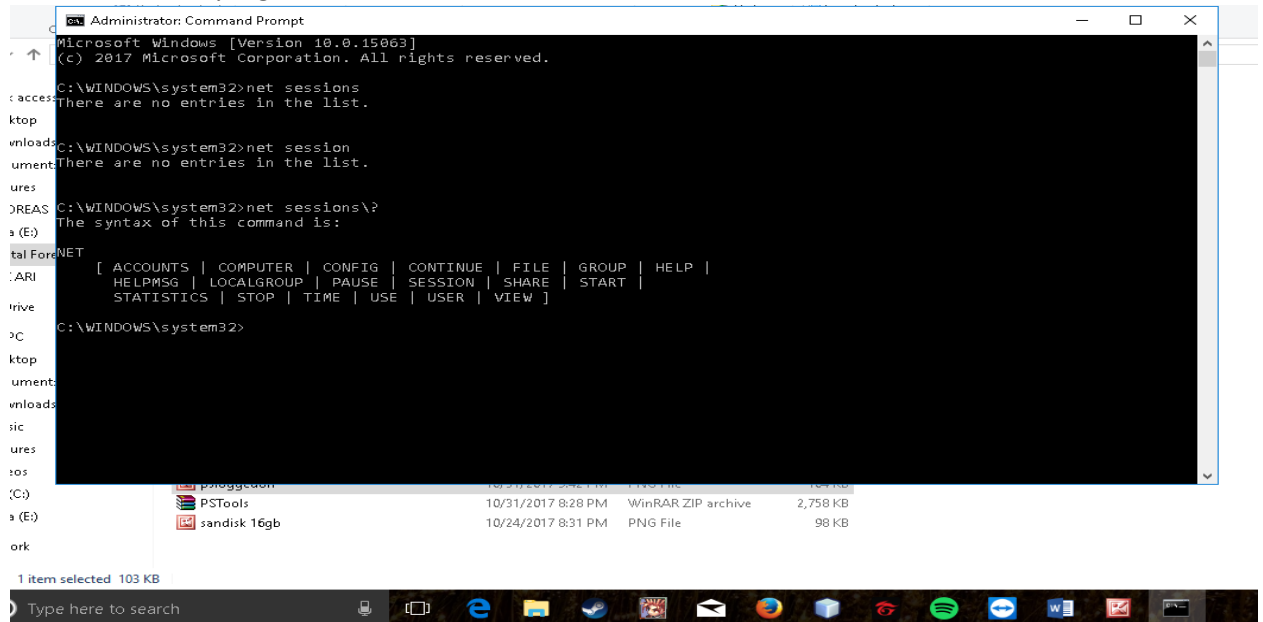
2. PSLOGGEDONON TOOL

Perintah ini menggunakan tools khusus yang harus di download terlebih dahulu melalui website dari Microsoft. Perintah ini digunakan untuk menampilkan nama dari user yang sedang login melalui remote.



3. NET SESSIONS

Perintah ini digunakan untuk mendapatkan informasi tentang username dan IP yang bias digunakan untuk mengakses sebuah system dengan menggunakan remote login session dan tipe dari sebuah client yang diakses.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>net sessions
There are no entries in the list.

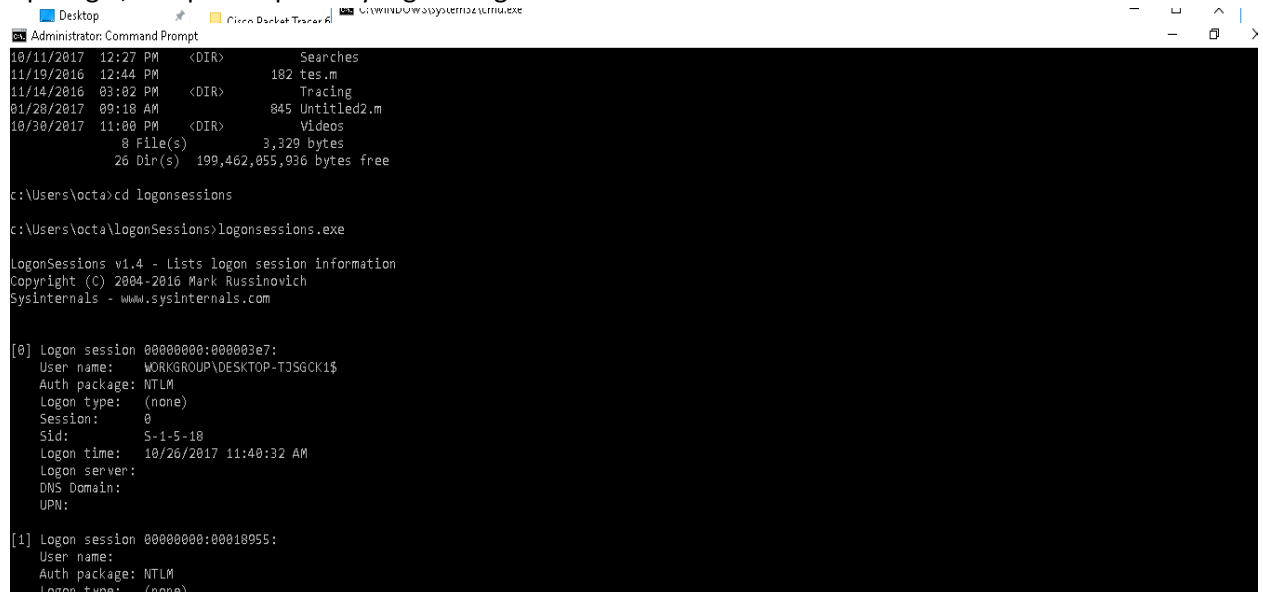
C:\WINDOWS\system32>net session
There are no entries in the list.

C:\WINDOWS\system32>net sessions\?
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:\WINDOWS\system32>
```

4. LOGONSESSIONS TOOLS

Perintah ini menggunakan tools khusus yang harus di download terlebih dahulu melalui website dari Microsoft. Perintah ini digunakan untuk menampilkan list dari paket-paket yang digunakan, tipe login, dan proses-proses yang sedang aktif.



```
Administrator: Command Prompt
10/11/2017 12:27 PM <DIR> Searches
11/10/2016 12:44 PM 182 tes.m
11/14/2016 03:02 PM <DIR> Tracing
01/28/2017 09:18 AM 845 Untitled2.m
10/30/2017 11:00 PM <DIR> Videos
8 File(s) 3,329 bytes
26 Dir(s) 199,462,055,936 bytes free

C:\Users\octa>cd logonSessions
C:\Users\octa\logonSessions>logonSessions.exe

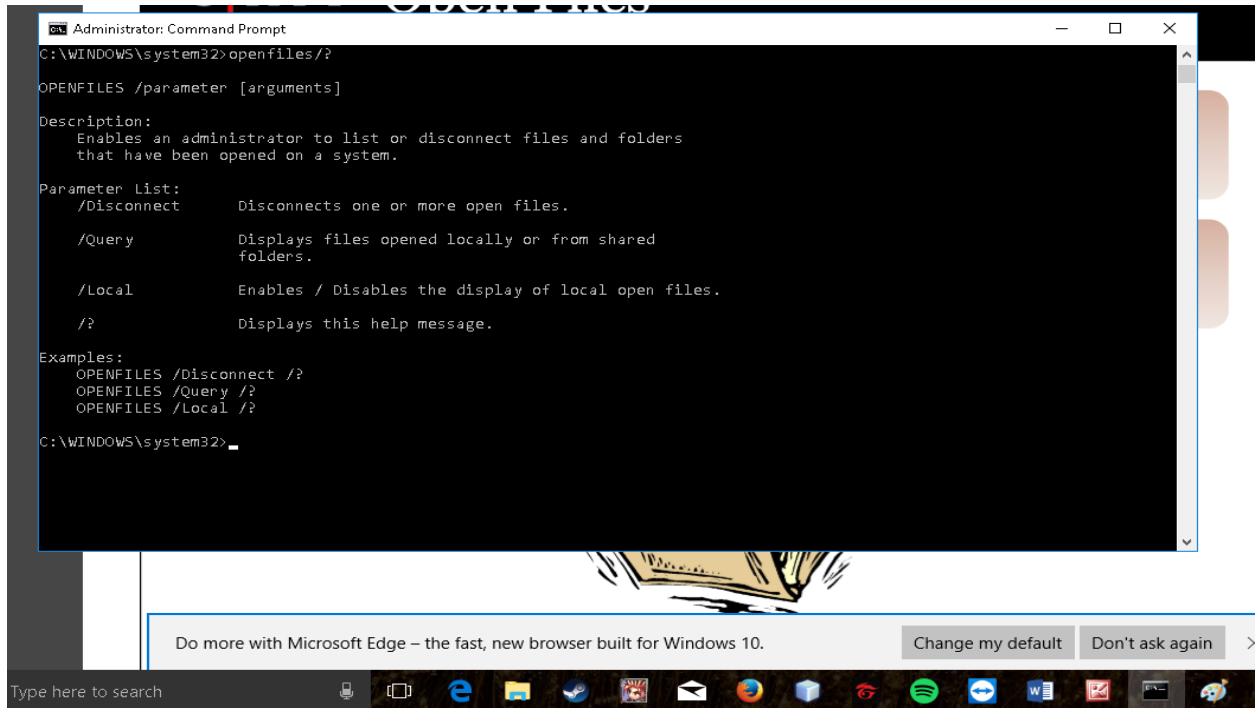
LogonSessions v1.4 - Lists logon session information
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
User name: WORKGROUP\DESKTOP-TJSGCK1$
Auth package: NTLM
Logon type: (none)
Session: 0
Sid: S-1-5-18
Logon time: 10/26/2017 11:40:32 AM
Logon server:
DNS Domain:
UPN:

[1] Logon session 00000000:00010955:
User name:
Auth package: NTLM
Logon type: (none)
```

5. OPEN FILES

Perintah ini digunakan untuk mengeksekusi sebuah file.



The screenshot shows a Windows 10 desktop. In the foreground, there is a Microsoft Edge browser window with the address bar showing a file path: `file:///E:/Octa/Kuliah/Digital%20Forensic/CHF1%20v4%20Module%2012%20Windows%20Forensics%20I.pdf`. Below the browser window, a taskbar is visible with various application icons. In the background, an Administrator Command Prompt window is open, displaying the help text for the `openfiles` command.

```
Administrator: Command Prompt
C:\WINDOWS\system32>openfiles/?

OPENFILES /parameter [arguments]

Description:
  Enables an administrator to list or disconnect files and folders
  that have been opened on a system.

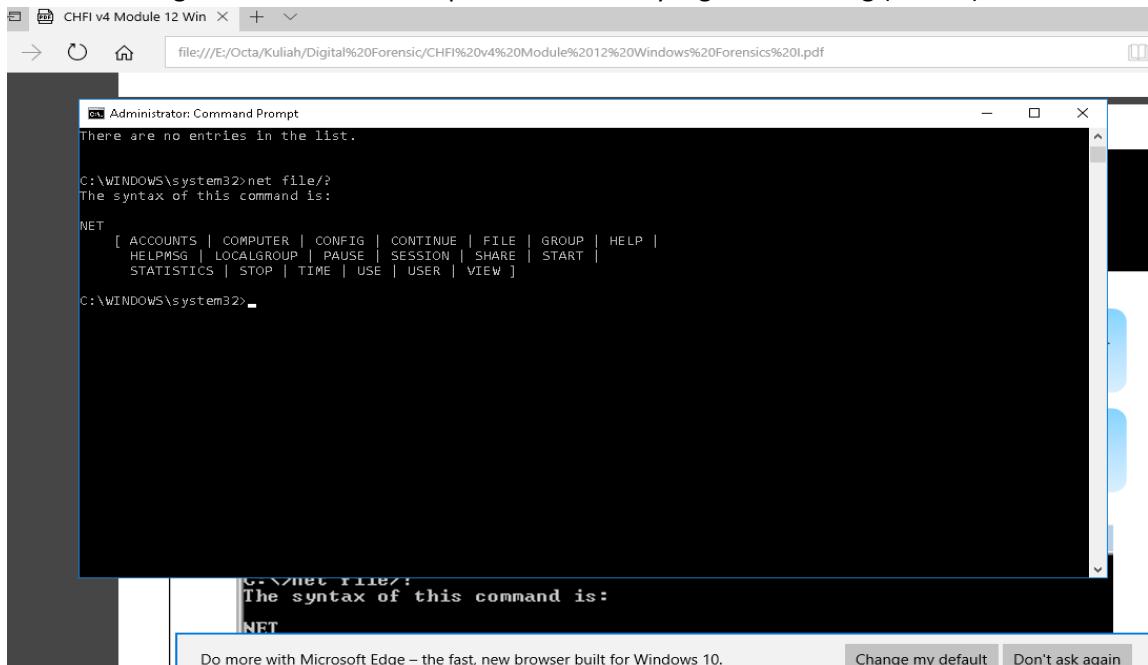
Parameter List:
  /Disconnect      Disconnects one or more open files.
  /Query           Displays files opened locally or from shared
                  folders.
  /Local           Enables / Disables the display of local open files.
  /?              Displays this help message.

Examples:
  OPENFILES /Disconnect /?
  OPENFILES /Query /?
  OPENFILES /Local /?

C:\WINDOWS\system32>
```

6. NET FILE

Perintah ini digunakan untuk menampilkan semua file yang sudah terbagi(shared).



The screenshot shows a Windows 10 desktop. In the foreground, there is a Microsoft Edge browser window with the address bar showing a file path: `file:///E:/Octa/Kuliah/Digital%20Forensic/CHF1%20v4%20Module%2012%20Windows%20Forensics%20I.pdf`. Below the browser window, a taskbar is visible with various application icons. In the background, an Administrator Command Prompt window is open, displaying the help text for the `net file` command.

```
Administrator: Command Prompt
There are no entries in the list.

C:\WINDOWS\system32>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:\WINDOWS\system32>
```