

## CLDFS

### LDFS

Tool Desc Live-data acquisition tools based Command Line  
Using Env Windows 2000, 2003, XP, Vista, 2008, 7

Contact park785@korea.ac.kr

### CLDFS

Download [CLDFS\(Freeware\)](#)

Hash(SHA1) 66decf5919fff3888e851010555dd7ad153a0950

### REGA

Live-data acquisition tools based Command Line

### WEFA

CLDFS is the live-data acquisition tool which is made from live-system acquisition function extracted in LDFS by DFRC. This tool is useful when a user wants to collect only volatile data, because it minimizes the changes on memory by removing GUI. The results are created as a RTF form report in the folder selected by a user, so it can be a reference for inspectors to write a report. The collected information by CLDFS is as follows.

### JPEGViewer

Basic Information

### P.F.P

- Case Information
- Acquisition Logs

### LNK Parser

System Information

- OS Info
- HDD Info

### Volafox

- Partition Info
- IP Info

User Account Information

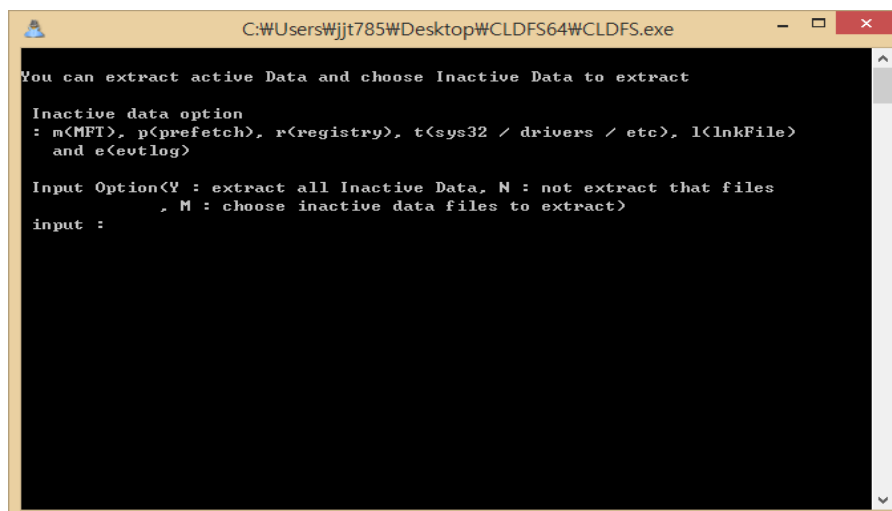
- All users
- Logged on user Info

Process Information

- Running processes
- DLL loaded on the system

Network Information

- Network Interfaces(NIC)
- Routing Table
- ARP Table
- Listening TCP/IP Ports
- Neighbor System in the same domain (NET VIEW)
- Shared Resource Info(NET SHARE)
- Remote User Info
- Remote resource that User is using(NET USE)



```

C:\Users\Wjjt785W\Desktop\CLDFS64\CLDFS.exe
You can extract active Data and choose Inactive Data to extract

Inactive data option
: m<MFT>, p<prefetch>, r<registry>, t<sys32 / drivers / etc>, l<lnkFile>
and e<evtlog>

Input Option<Y : extract all Inactive Data, N : not extract that files
, M : choose inactive data files to extract>
input :
  
```

