Digital Forensics
KOREA UNIVERSITY

LDFS
CLDFS
REGA
WEFA
JPEGViewer
P.F.P
LNK Parser
Volafox

CLDFS

Tool Desc	Live-data acquisition tools based Command Line
Using Env	Windows 2000, 2003, XP, Vista, 2008, 7
Contact	park7 85@korea.ac.kr
Download	CLDFS(Freeware)
Hash(SHA1)	66decf5919fff3888e851010555dd7 ad153a0950

Live-data acquisition tools based Command Line

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.

Basic Information

- Case Information
- Acquisition Logs

System Information

- OS Info
- HDD Info
- 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
- Listenning 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)