Digital Forensics
KOREA UNIVERSITY

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

REGA

Tool Desc	Windows Registry Analyzer
Using Env	Windows NT / 2000 / XP / 2003 / 2008 / VISTA / 7 / 8 (consumer preview)
Contact	Any problem, suggestion, comment, found a bug in this program, contact to chjs207@gmail.com
Lite version download	TBA
Lite version	The lite version has some functional restrictions.
For commercial ver	http://www.4n6tech.com/
Download	REGA(Freeware)
Hash(SHA1)	e601397f9e8f1643bb6dcfbc94b474fc45f73935

REGA

REGA is the forensic tool performing collection and analysis of the windows registry hives (GUI application)

RegEx

Console application for collecting registry hive files.

Supported platforms

Windows (written in C/C++ and MFC)

Language

Korean, English, Japanese

Features

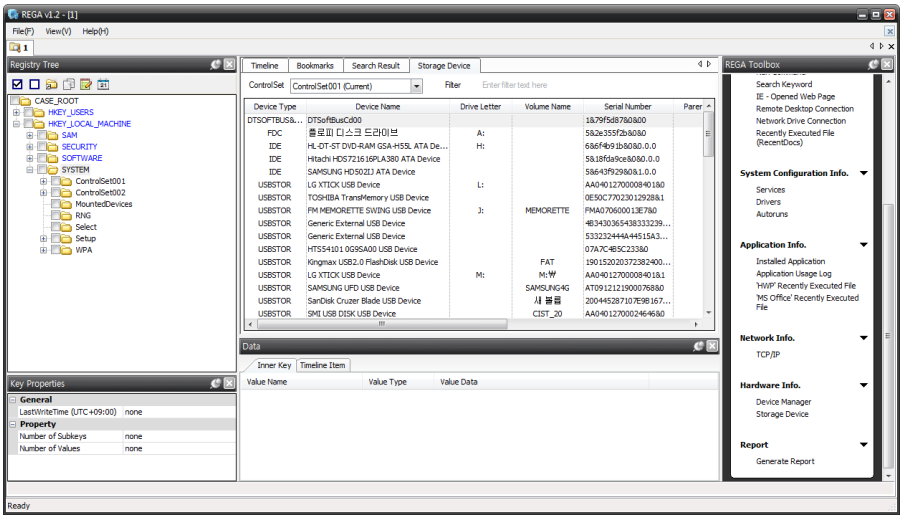
- Intuitive GUI based application
- Automatically search a target computer and quickly collect registry hive files (using RegEx)
- Extract forensicically meaningful information in pre-defined categories
- Decrypt and decode registry data to enhance the readabiilty
- Rapid search with keywords and time preriods
- Timeline analysis
- Create result reports (CSV format)

Functions

- Automatically search a target computer and quickly collect registry hive files (using RegEx)
- Recovery deleted registry data (key, value and data)
- Analyze windows installation information including
  - Owner, Organization, Installation date, and so on
- Analyze user activities such as
  - User accounts, Protected storage, Run commands, Search keywords
  - Typed URLs of internet explorer
  - Remote desktop connection, Network drive connection
  - Recently accessed folders and files
- Analyze system configuration information such as
  - List of services and drives
  - Autoruns
- Analyze installed application and the usage history
  - Installed application, Application usage history
  - Application compatibility cache
  - Word process application usage history (Microsoft office 1997-2010 and Haansoft hangle 2000-2010)
- Analyze installed hardware and the usage history
  - Installed network interface cards
  - Installed hardware (device managers)
  - Installed storage devices (hdd, fdd, cd-rom, usb ...)
- Reporting
  - Create result reports (analyzed information is saved in the CSV file format)

Sponsored by

- CIST (Center for Information Security Technologies)
- DFRC (Digital Forensics Research Center)
- FORENSIC INSIGHT



Center for information Security Technologies. Anam-dong 5-ga Seongbu-gu, Seoul, Korea. / TEL +82-2-3290-4738 / FAX +82-2-928-9109