Win-LiFT

Windows Live Forensic Tool

Win-LiFT is a Windows Live Forensics Tool consisting of Win-LiFTImagerBuilder and Win-LiFTAnalyzer. Live Forensics involves acquisition of volatile data from the Suspect's machine and analysis of the acquired data. Win-LiFT enables volatile data acquisition using Win-LiFTImager and analysis of the same using Win-LiFTAnalyzer.

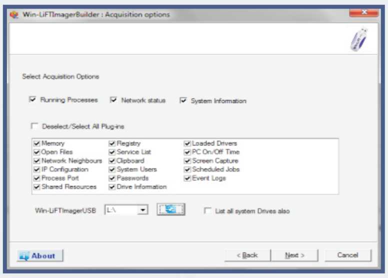
Win-LiFTImagerBuilder

Tool for building Win-LiFTImager

Win-LiFTImagerBuilder, which runs in the Investigator's machine, builds Win-LiFTImager tool.

Features

- Facility to enter crime details
- Facility to select / deselect the list of volatile artifacts to be collected from the Suspect's system
- Facility to select USB/Hard Disk drive to which Win-LiFTImager tool is to be built



Win-LiFTImagerBuilder : Acquisition options

Select Acquisition Options

☑ Running Processes ☑ Network status ☑ System Information

☐ Deselect/Select All Plug-ins

☑ Memory	☑ Registry	☑ Loaded Drivers
☑ Open Files	☑ Service List	☑ PC On/Off Time
☑ Network Neighbours	☑ Clipboard	☑ Screen Capture
☑ IP Configuration	☑ System Users	☑ Scheduled Jobs
☑ Process Port	☑ Passwords	☑ Event Logs
☑ Shared Resources	☑ Drive Information	

Win-LiFTImagerUSB L:\

☐ List all system Drives also

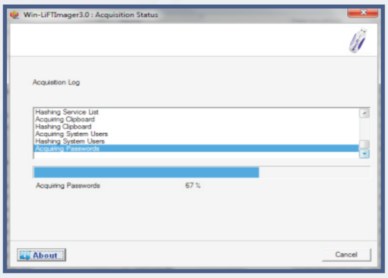
Win-LiFTImager

Forensic Volatile Data Acquisition Tool

Win-LiFTImager is a USB based tool for Live Forensics Data Acquisition from Suspect's machine.

Features

- Capturing following volatile artifacts from the Suspect's machine to the Win-LiFTImager USB.
  - Running Processes
  - Network Neighbors
  - Process Port Connections
  - Routing Table
  - Scheduled Jobs
  - Services List
  - System Users
  - Drive Information
  - Installed Applications
  - Printer Information
  - Bluetooth Device Details
  - System Information
  - Network Connection
  - Open Files
  - Network Interfaces
  - Shared Resources
  - Clipboard Content
  - PC On/Off Time
  - Loaded Drivers
  - Recycle Bin Information
  - USB Information
  - Jump Lists



Win-LiFTImager3.0 : Acquisition Status

Acquisition Log

```
Hashing Service List
Acquiring Clipboard
Hashing Clipboard
Acquiring System Users
Hashing System Users
Acquiring Passwords
```

Acquiring Passwords 67 %

- Facility to dump Physical Memory content from Windows Systems
- Facility to capture Snapshot of Desktop Screen from the Suspect's machine
- Acquires Registry Files and Browser Files from Windows Systems
- Acquisition of Event Log files
- Hashing of all acquired files
- Log and Report Generation

Win-LiFT

Windows Live Forensic Tool

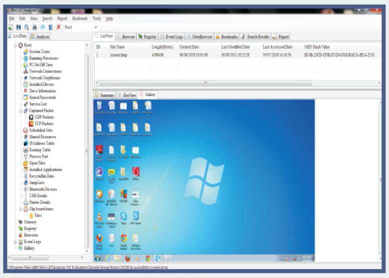
Win-LiFTAnalyzer

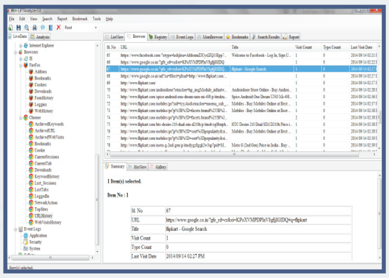
Forensic Volatile Data Analysis Tool

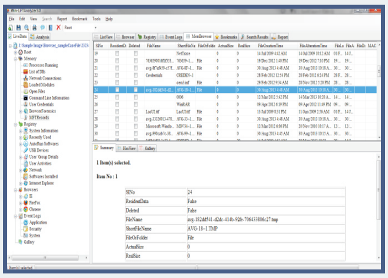
Win-LiFTAnalyzer analyses the data collected by the Win-LiFTImager and creates a detailed report after analysis.

Features

- Analyze the Live Forensics data captured by Win-LiFTImager from the Suspect's machine
- Advanced Memory Analysis from Windows XP and Windows 7 Physical Memory dump to extract the following forensically sound information
  - Running Process and its associated details
  - Network Information
  - User Credentials
  - Internet usage based Information
  - MFT Records
  - Executable Reconstruction
- Structural Analysis of Reconstructed Executables
- Registry Analysis to retrieve forensically relevant information
- Event Log Analysis
- Browser Forensics of IE, Chrome and Firefox
- Keyword Searching facility
- Detailed Report Generation
- Bookmarking and appending to Report facility
- Facility to save and print Report
- Facility to save partially/fully analyzed cases
- Handling multiple case files(.cfs) simultaneously
- Independent Loading and analysis of Registry Files and Memory dump
- Hash Verification of acquired information







Other Features

- Display forensic evidence acquired in List/Tree/Summary View.
- Gallery View and Summary view
- Text-Hex View of raw files with built-in search and go to facility.
- Parent-Child view of Running processes

www.cdac.in

CYBER SECURITY GROUP
Centre for Development of Advanced Computing
R&D Organization of Ministry of Electronics and Information Technology
Govt. of India
Vellayambalam, Thiruvananthapuram - 695 033, Kerala State, India
Phone: +91 471 2723333, 2728929, 2727004 / Fax: +91 471 2723456
Email: cyber-tvm@cdac.in, Web: www.cyberforensics.in
Help Desk: https://servicedesk.cyberforensics.in/