LAB MANUAL
ON
WinLiFT ImagerBuilder TOOL

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

Table of Contents

MANUAL-9:

WinLiFT IMAGER-BUILDER TOOL

INTRODUCTION TO DIGITAL FORENSICS

- It is a process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.
- Basically Digital Forensics is a science of finding evidence from digital media such as:
  - Computers
  - Smart phones
  - Servers
  - Networks
- In Digital Forensics, dead analysis is performed on static data either from a core dump or do bit-to-bit imaging. For example, to pull the plug of all computer systems involved and analyze an image of the hard drives.
- In contrast, live analysis is data collection on systems that are still running. It considers the value of the data that may be lost by powering down a system. It extracts “live” system data before pulling the cord to preserve memory, process, and network information.
- In Digital Forensics, volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off.

- Volatile data resides in registries, cache, and random access memory (RAM). The investigation of this volatile data is called “live forensics”.

INTRODUCTION TO WINLIFT

- WinLiFT stands for Windows Live Forensics Tool.
- WinLiFT is a live forensics acquisition tool, developed by Cyber Security Group, Centre for Development of Advanced Computing (C-DAC) Thiruvananthapuram.
- It is used for the acquisition of a volatile data from a computer system in on state. It collects and stores data directly onto the USB.
- WinLiFT v3.0 consists of:
  - WinLiFT ImagerBuilder Tool
  - WinLiFT Analyzer Tool
- 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-LiFT ImagerBuilder tool and performs analysis using Win-LiFT Analyzer tool.

- In this manual, we will discuss Win-LiFT ImagerBuilder tool.

TOOL: WINLIFT IMAGERBUILDER TOOL

Win-LiFT ImagerBuilder v 3.0 is a USB based tool for Live Forensics Data Acquisition from Suspect's machine. It captures following volatile artifacts from the Suspect's machine to the Win-LiFT Imager USB:

- Running Processes
- Network Neighbours
- Open Files
- Process Port Connections
- Shared Resources
- Memory
- Registry
- Service List
- Clipboard Content
- System Users
- Drive Information
- Loaded Drivers
- PC on/off Time
- Screen Capture
- Scheduled Jobs

- Event Logs
- Packet Capture
- Installed Applications
- IP Configuration
- Recycle Bin
- Printer Info
- USB Information
- Bluetooth Device Details
- JumpLists

The features of WinLiFT ImagerBuilder Tool are as follows:

- It provides facility to dump Physical Memory content from Windows Operating Systems.
- It provides facility to capture Snapshot of Desktop Screen from the Suspect's machine.
- It acquires Registry Files and Browser Files from Windows Systems.
- It acquires Event Log files.
- It provides facility of MD5 hashing of all acquired files.
- It provides facility of Log and Report Generation.

HOW TO ACQUIRE DATA WITH WinLiFT IMAGERBUILDER TOOL

Step 1: Open WinLiFT ImagerBuilder Tool after installation as shown in Figure 1.

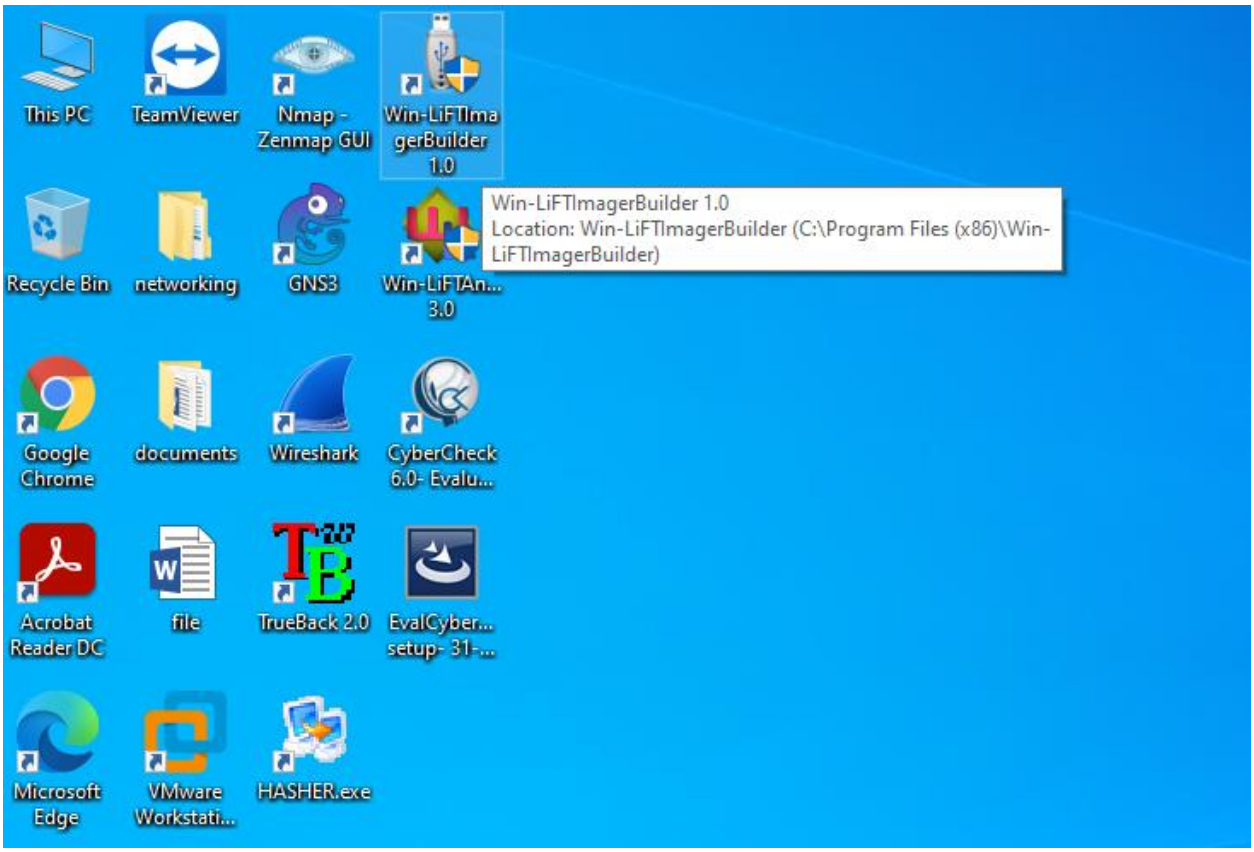

Figure 1: Open WinLiFT ImagerBuilder Tool

Step 2: Click "Next" button to enter the case details as shown in Figure 2.

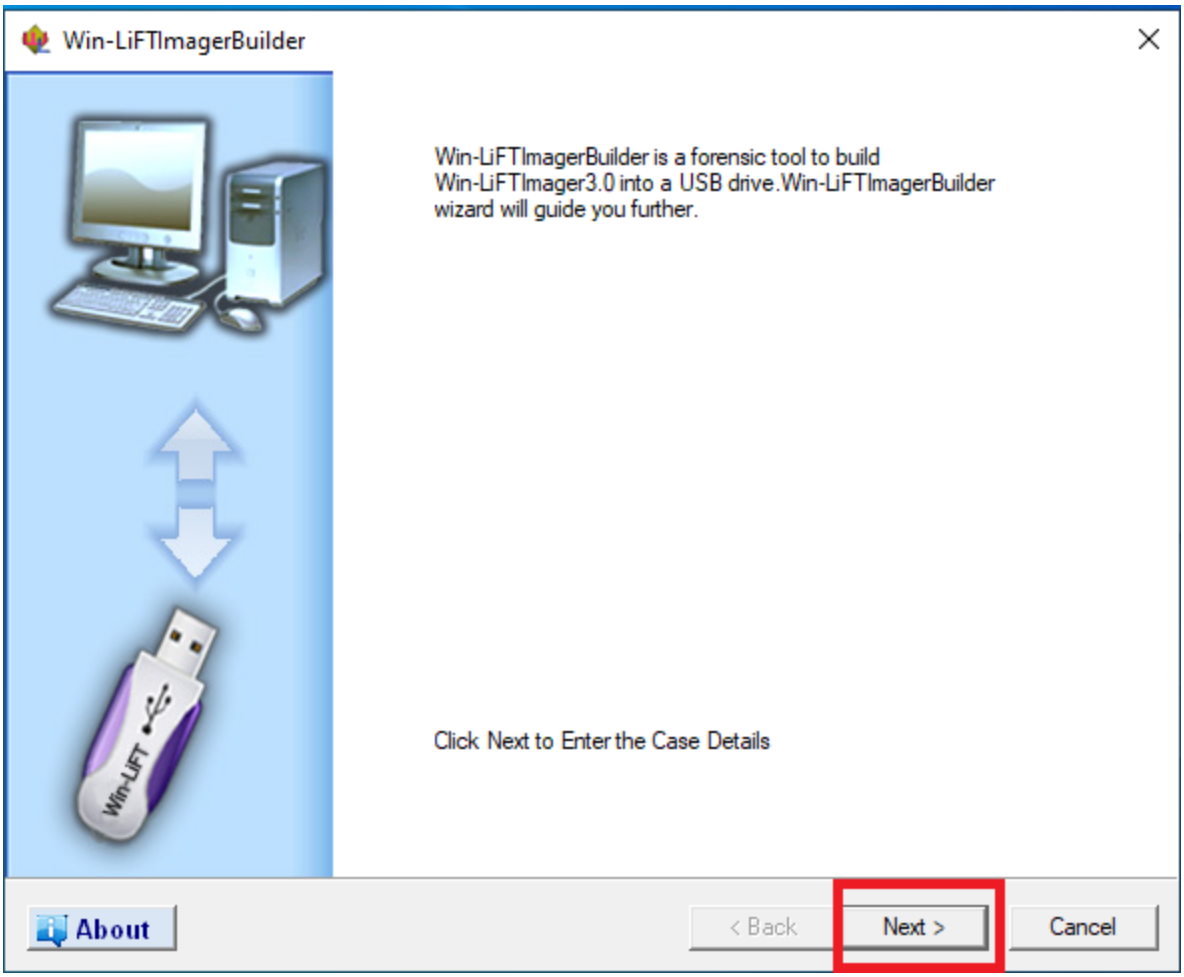

Figure 2: About WinLiFT ImagerBuilder Tool

Step 3: Enter the case details in the text box as shown in Figure 3. After filling the case details (Investigator's Name, Investigator's Rank, Police Station, Crime Number, Seizure Memo No, Place of Seizure, Name of Suspect, Address 1, and Address 2), click *Next* button as shown in Figure 4.

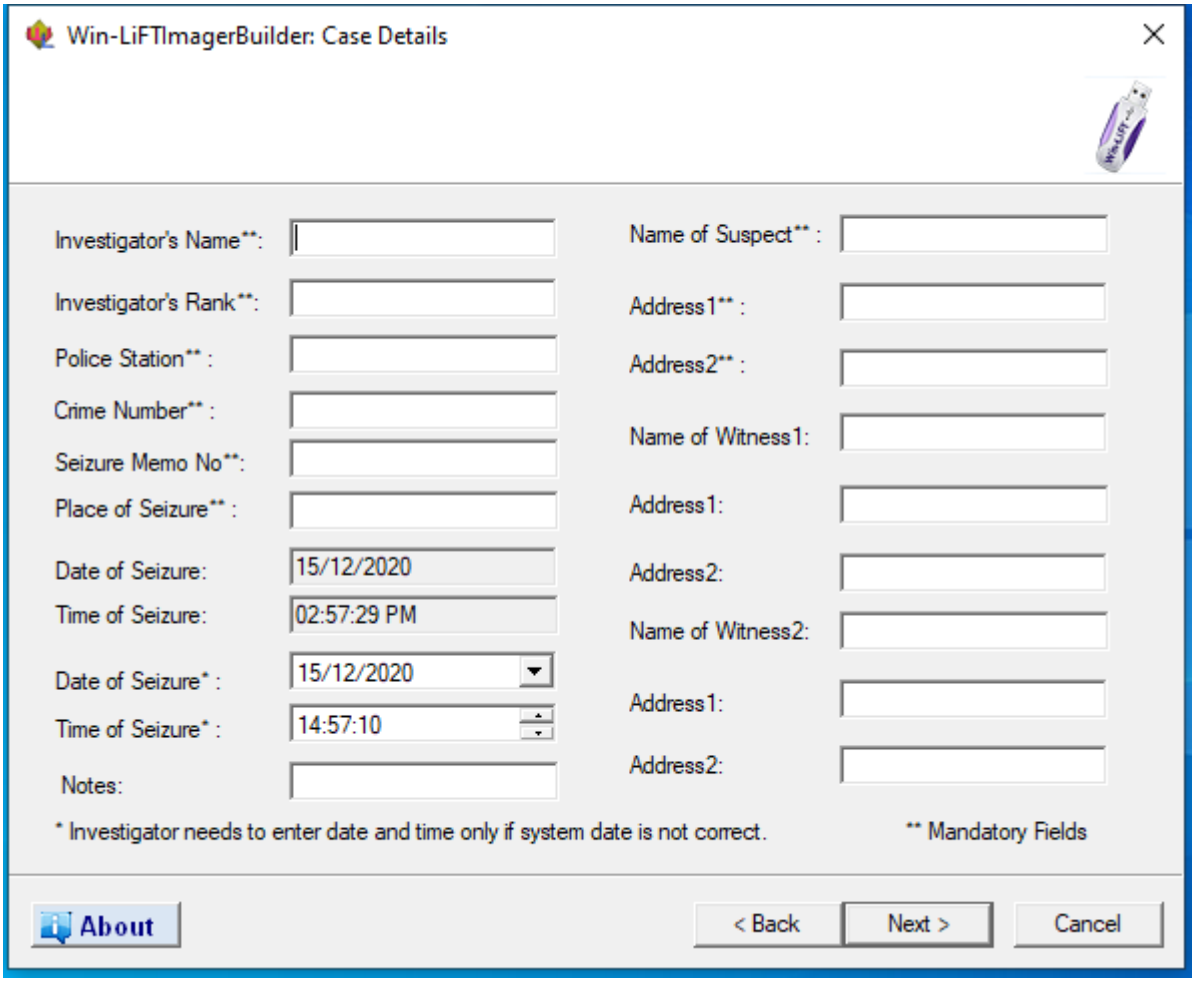

Figure 3: Enter the Case Details

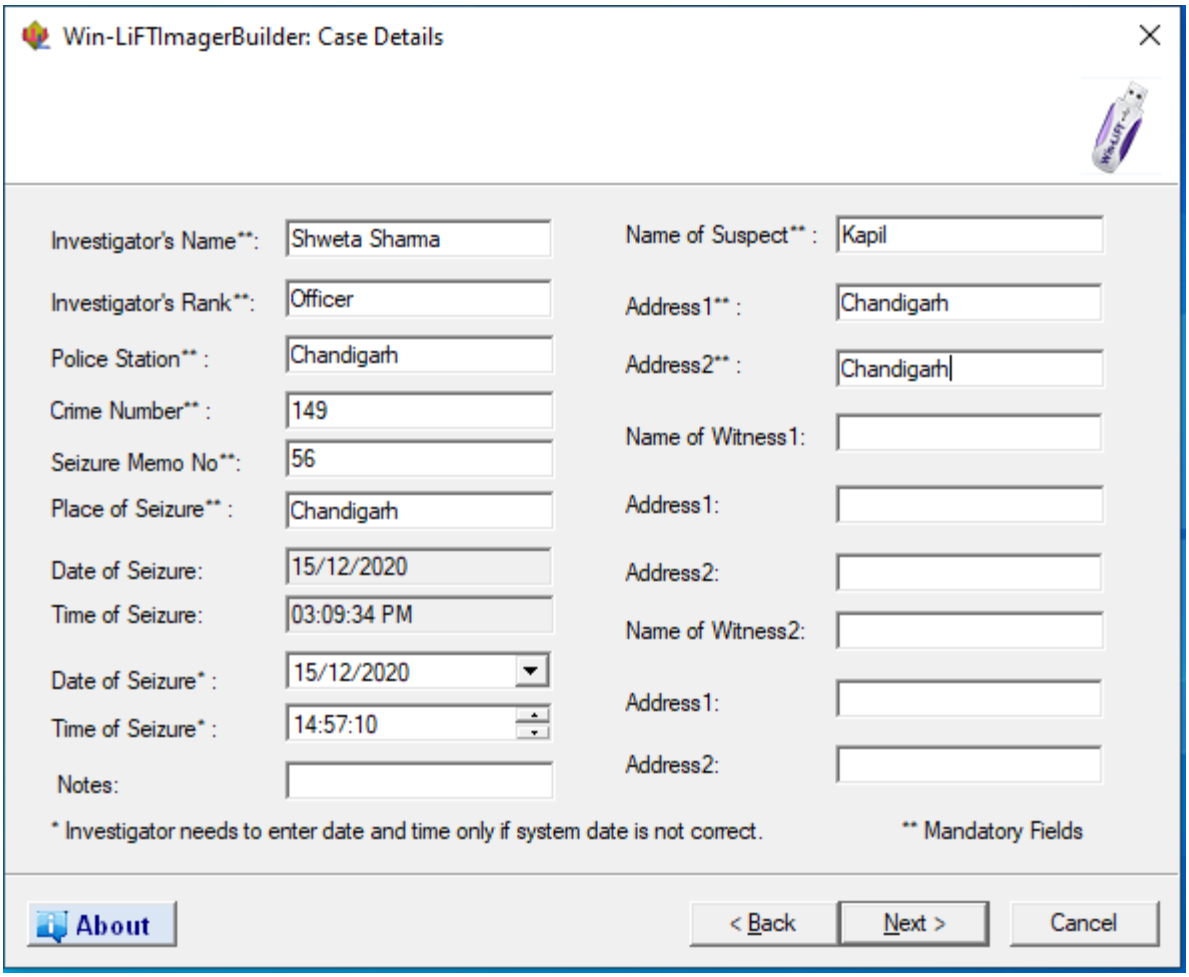

Figure 4: Press Next Button

Step 4: Select Volatile Artifacts to acquire from Suspect's Machine as shown in Figure 5. Select the USB drive from the drop-down box and click *Next* button as shown in Figure 5. Click *Yes* button to continue with the selected Win-LiFTImager USB drive (F:)as shown in Figure 6.

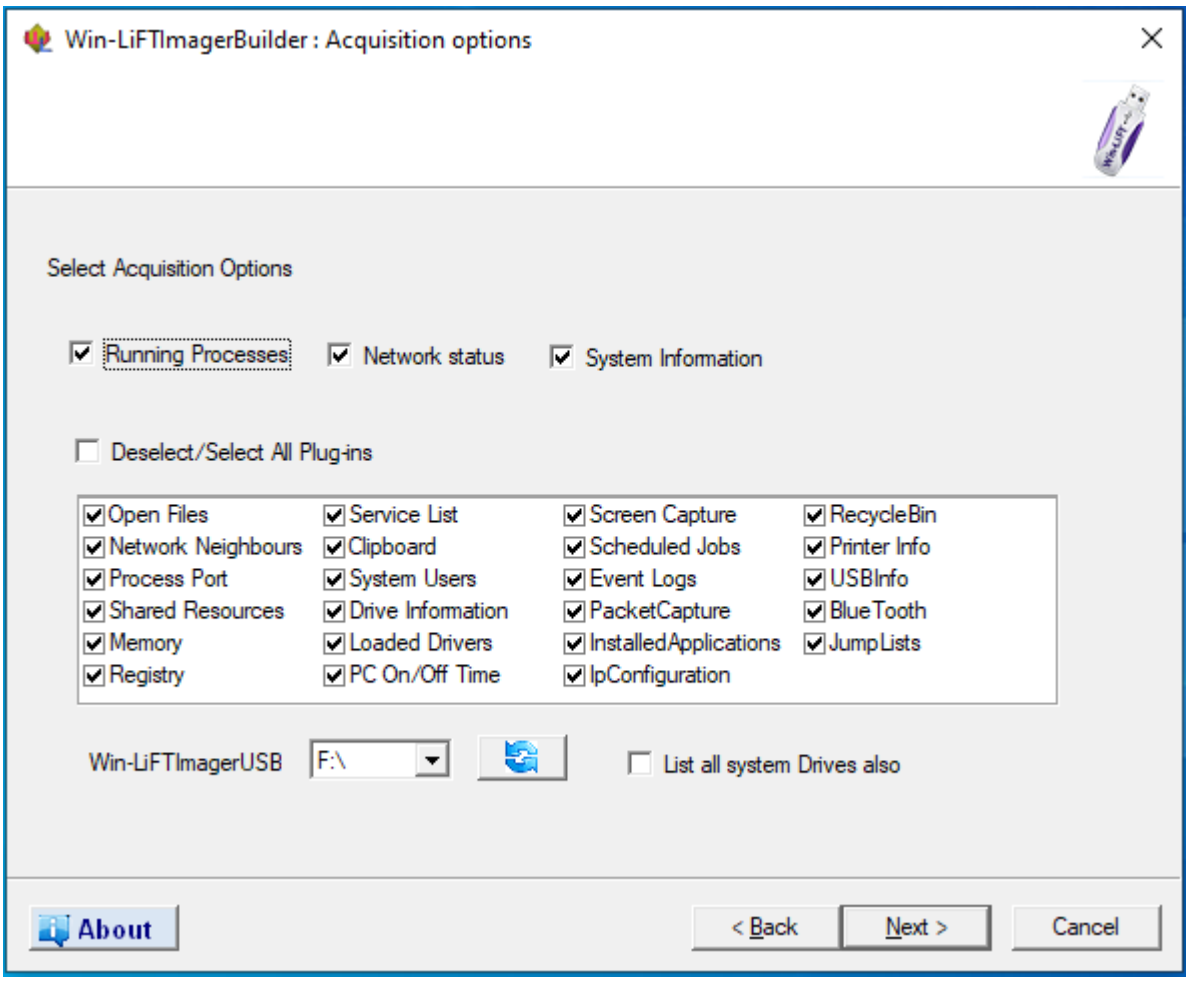

Figure 5: Select Volatile Artifacts from Suspect's Machine

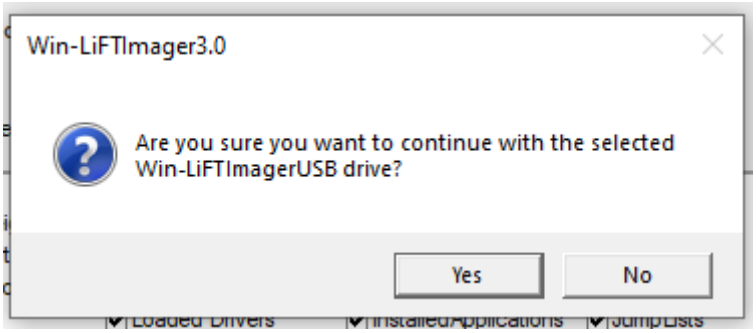

Figure 6: Press Yes Button

Step 5: The report of Volatile Artifacts will be displayed by WinLiFT ImagerBuilder tool. Click *Done* button to close the window as shown in Figure 7.

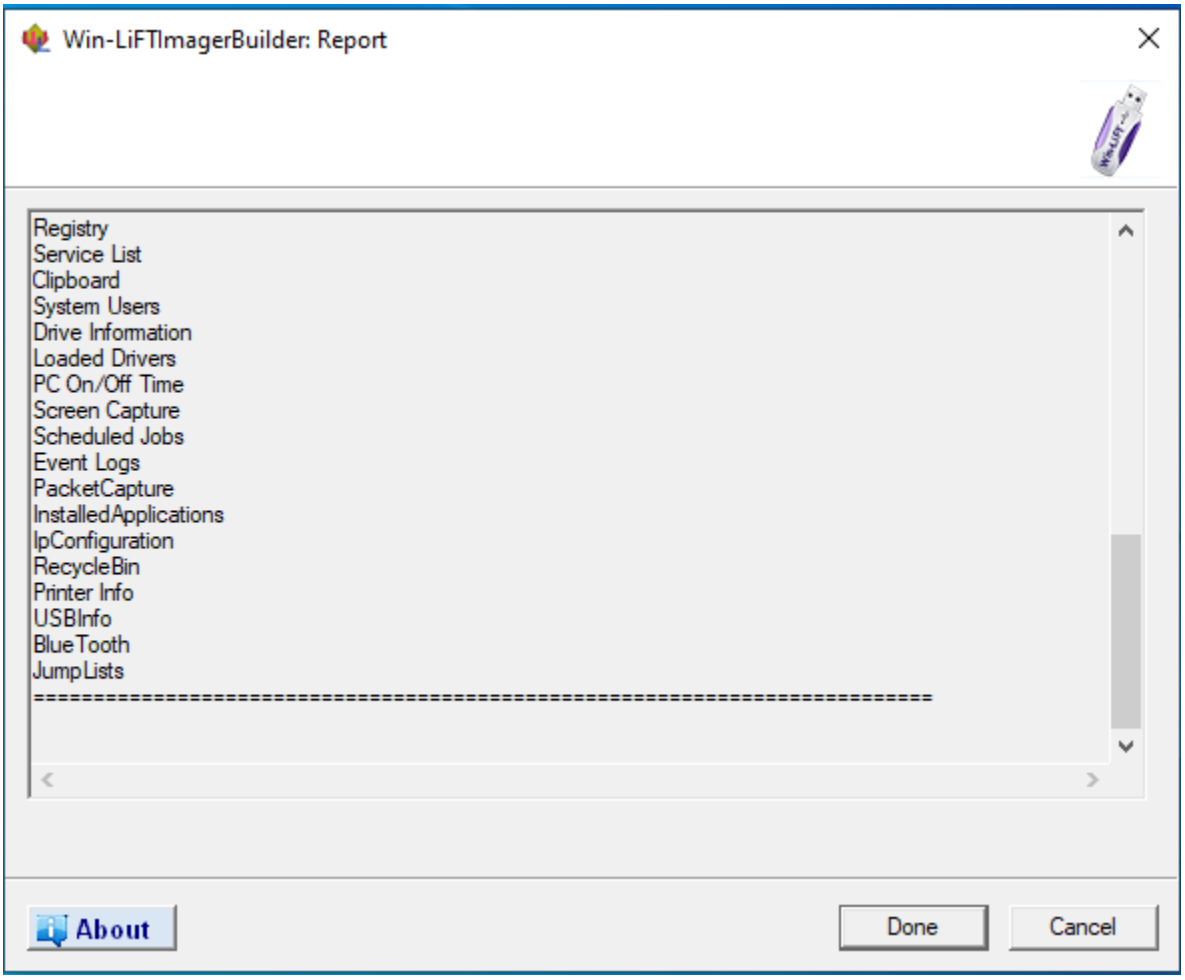

Figure 7: Report of WinLiFT ImagerBuilder Tool

Step 6: Go to the USB Drive (F:) and run Win-Lift Imager application as shown in Figure 8.

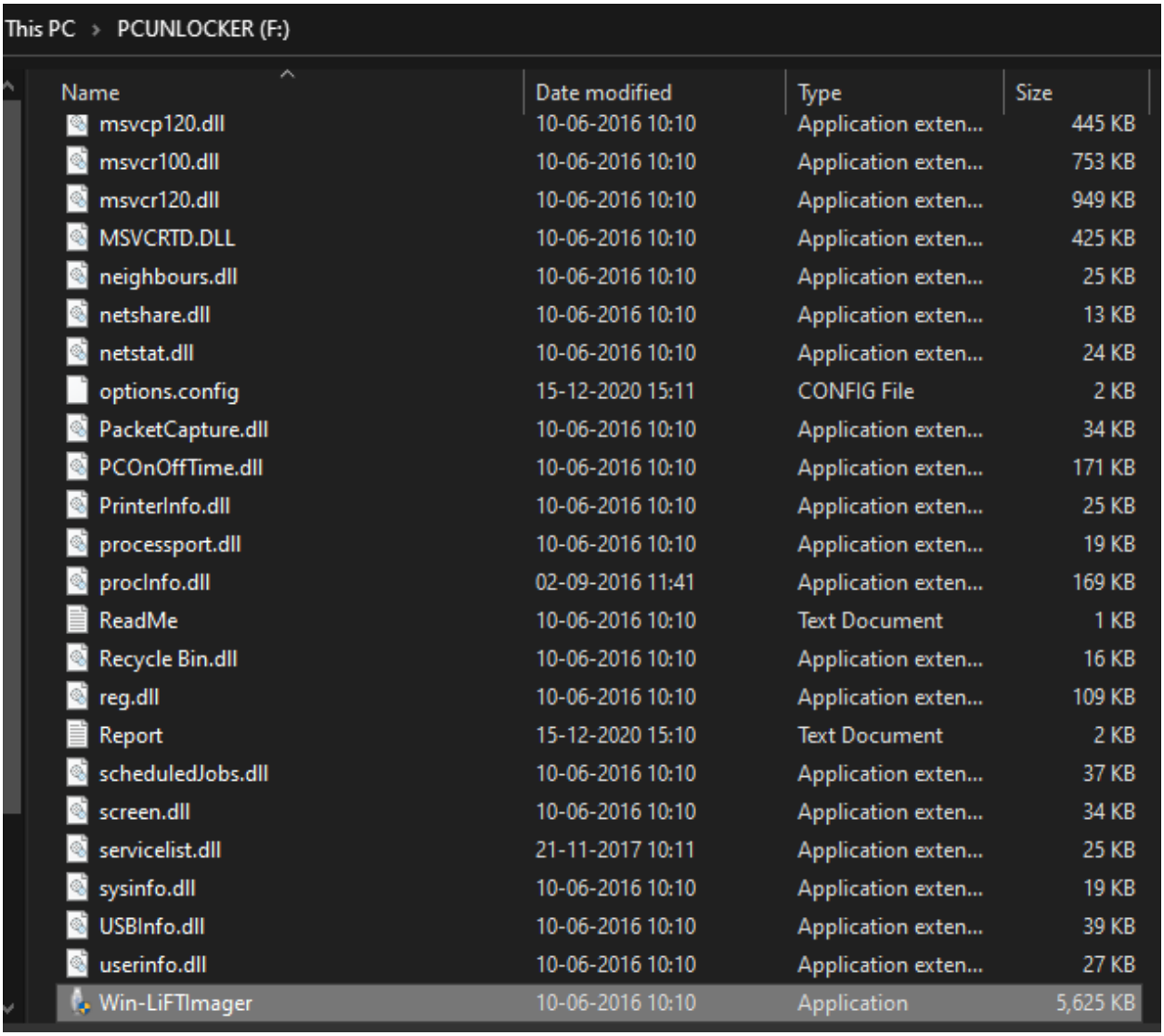

Figure 8: Run Win-LiFTImager Tool

Step 7: The acquisition status to acquire the volatile data will be displayed as shown in Figure 9.

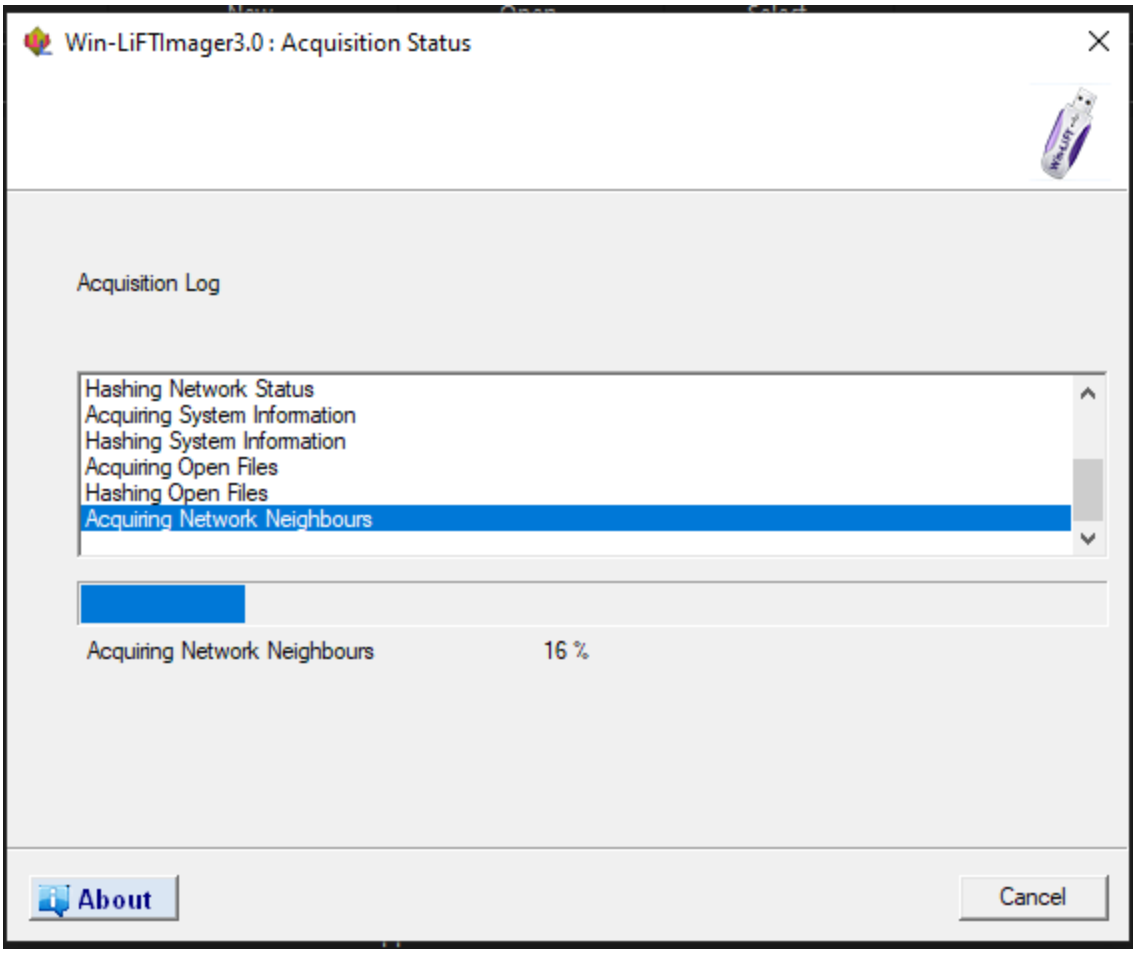

Figure 9: Acquisition Status

Step 8: A command prompt will open to ask about whether you want to dump memory or not. Type 'y' to continue as shown in Figure 10. It will show the status as progressing as shown in Figure 11. Once it is completed, the status will change to success as shown in Figure 12.

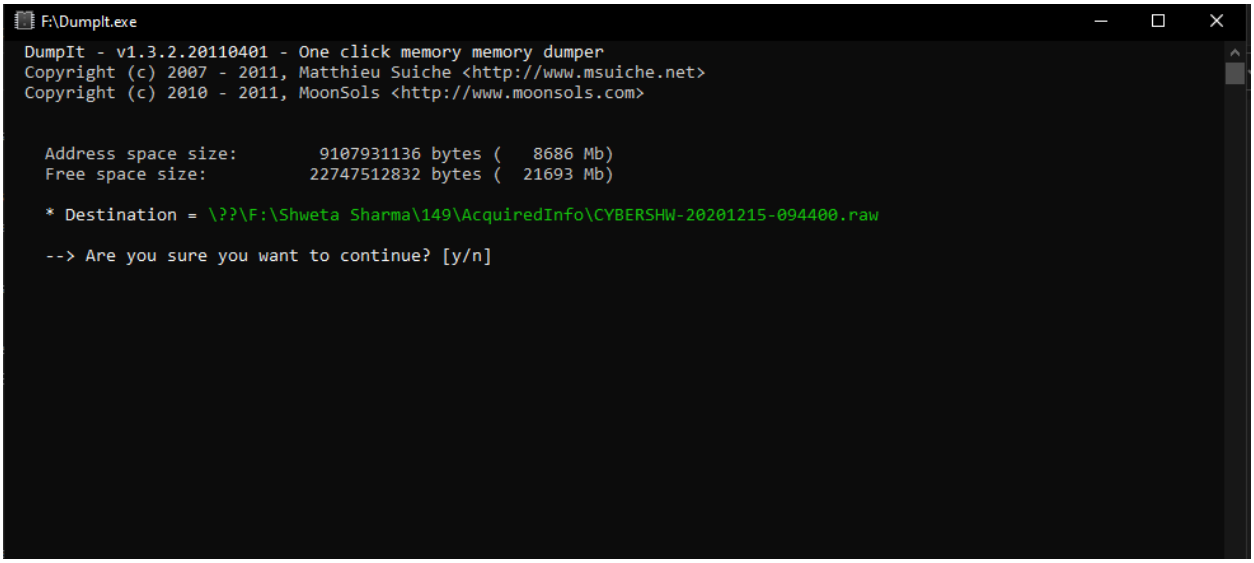

Figure 10: Memory Dump

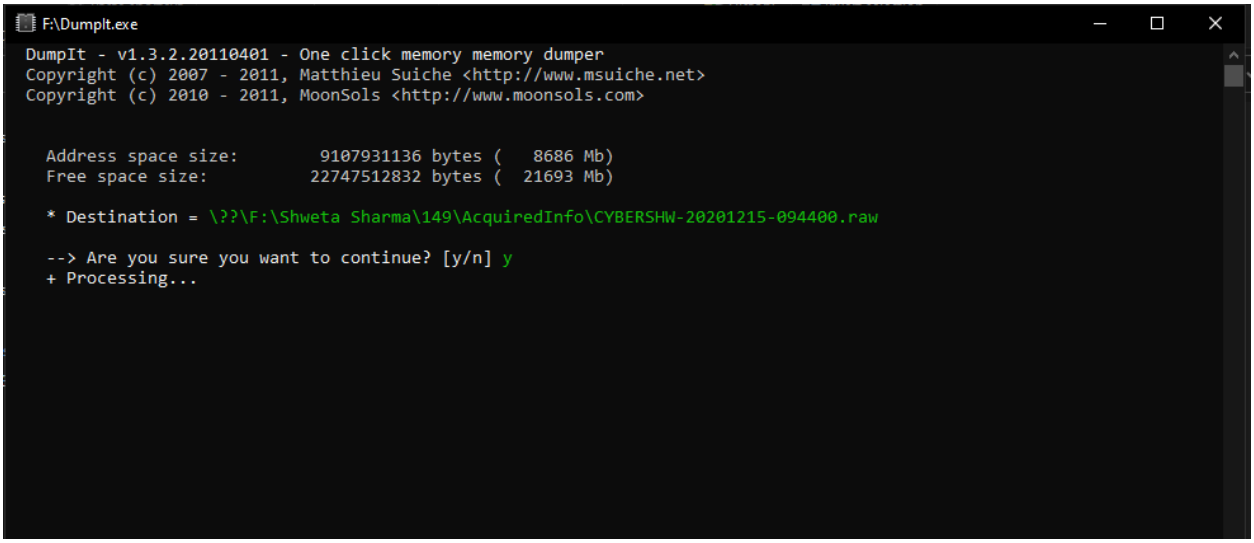

Figure 11: Memory Dump in Progress

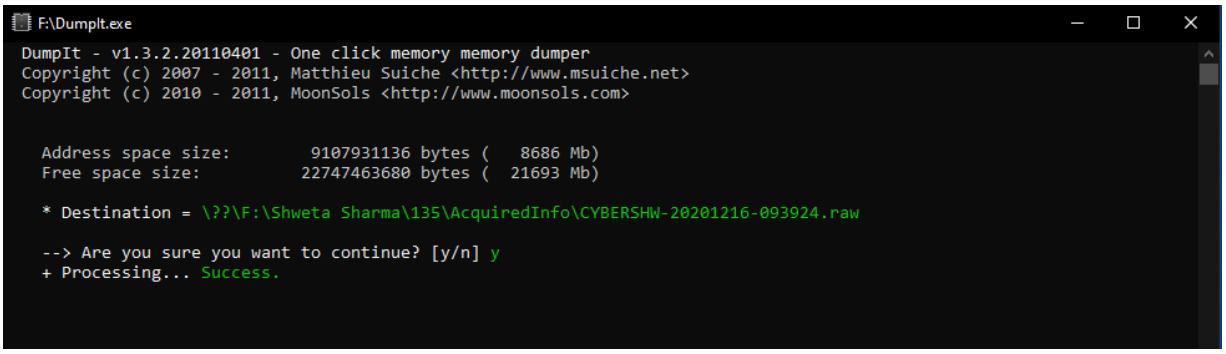

Figure 12: Memory Dump Completed

Step 9: Once the progress bar reaches to 100%, the data acquisition is completed as shown in Figure 13. The output of the WinLiFT ImagerBuilder tool will be analyzed by the WinLiFT Analyzer tool.

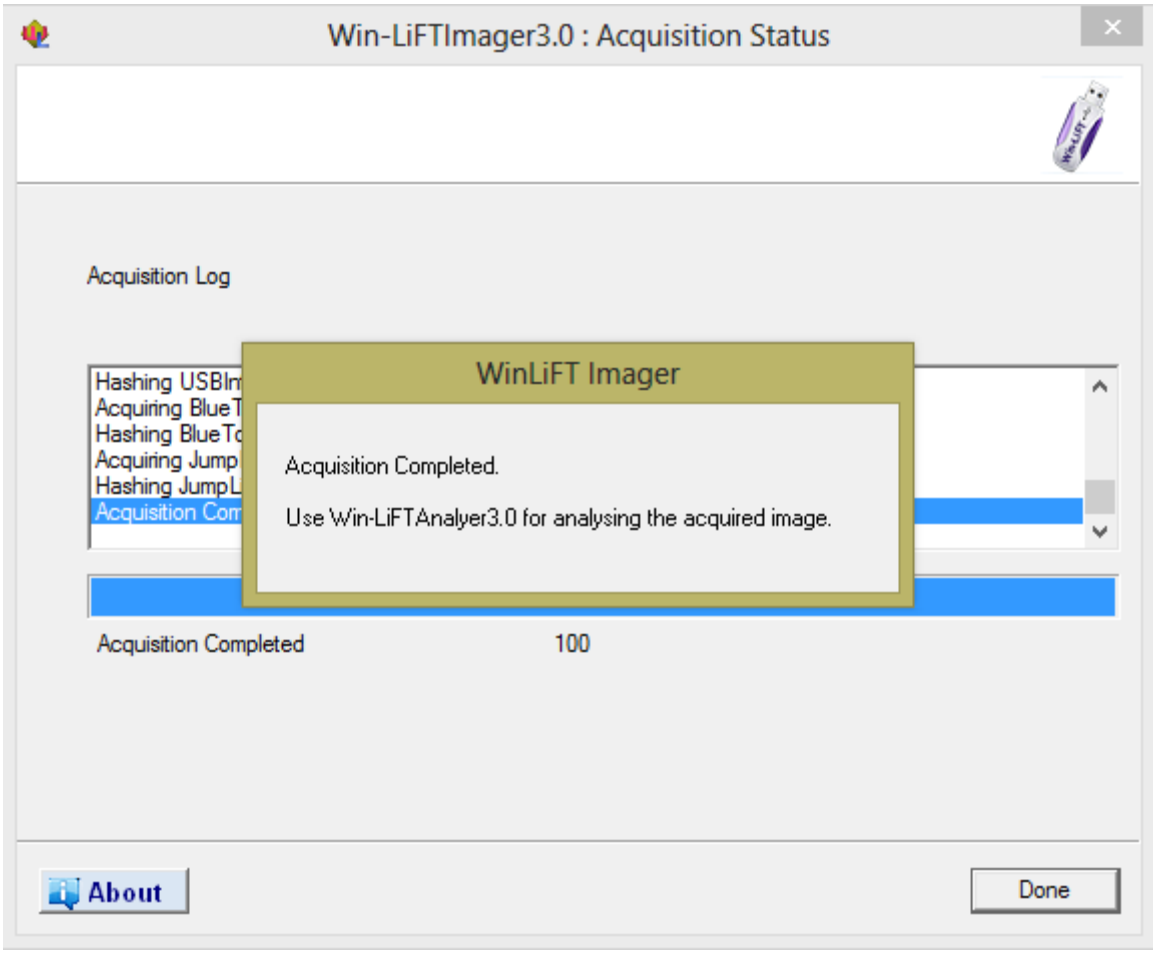

Figure 13: Data Acquisition Completed

REFERENCES

[1] Win-LiFT Windows Based Live Forensics Tool, 2021, https://www.cdac.in/index.aspx?id=cs_cf_CSG_WINLFT (accessed March 2, 2021).