LAB MANUAL
ON
WinLiFT ANALYZER 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-10:

WinLiFT

ANALYZER

TOOL

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 Analyzer tool.

TOOL: WINLIFT ANALYZER TOOL

Win-LiFT Analyzer v3.0 analyses the data collected by the Win-LiFTImager. It creates a detailed report after analysis

The features of Win-LiFT Analyzer tool are as follows:

- It analyzes the Live Forensics data captured by Win-LiFTImager form the suspect's system.
- It performs MD5 Hash Verification of acquired files.
- It performs Memory and Event Log Analysis.
- It performs Registry Analysis to retrieve forensically relevant information.
- It performs Event Log Analysis.
- It performs Browser Forensics.
- It performs Advanced Memory Analysis for Running Process Details, Network Information, Internet Evidence and MFT Records Collection.
- It generates a Detailed Report.
- It provides Bookmarking and Appending to report facility.
- It provides facility to save partially/fully analyzed cases.

- It provides facility to save and print report.
- It provides facility to load Windows Memory dump files .
- It displays forensic evidence acquired in List/Tree/Summary View.
- It provides Gallery View of the screenshot & clipboard images.
- It provides Text-Hex View of raw files with built in search and go to facility.
- It provides Tree view of the Running process.

HOW TO ANALYZE DATA WITH WinLiFT ANALYZER TOOL

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

Step 2: Click on File Tab as shown in Figure 2. Select a New Case File form the menu as shown in Figure 3.

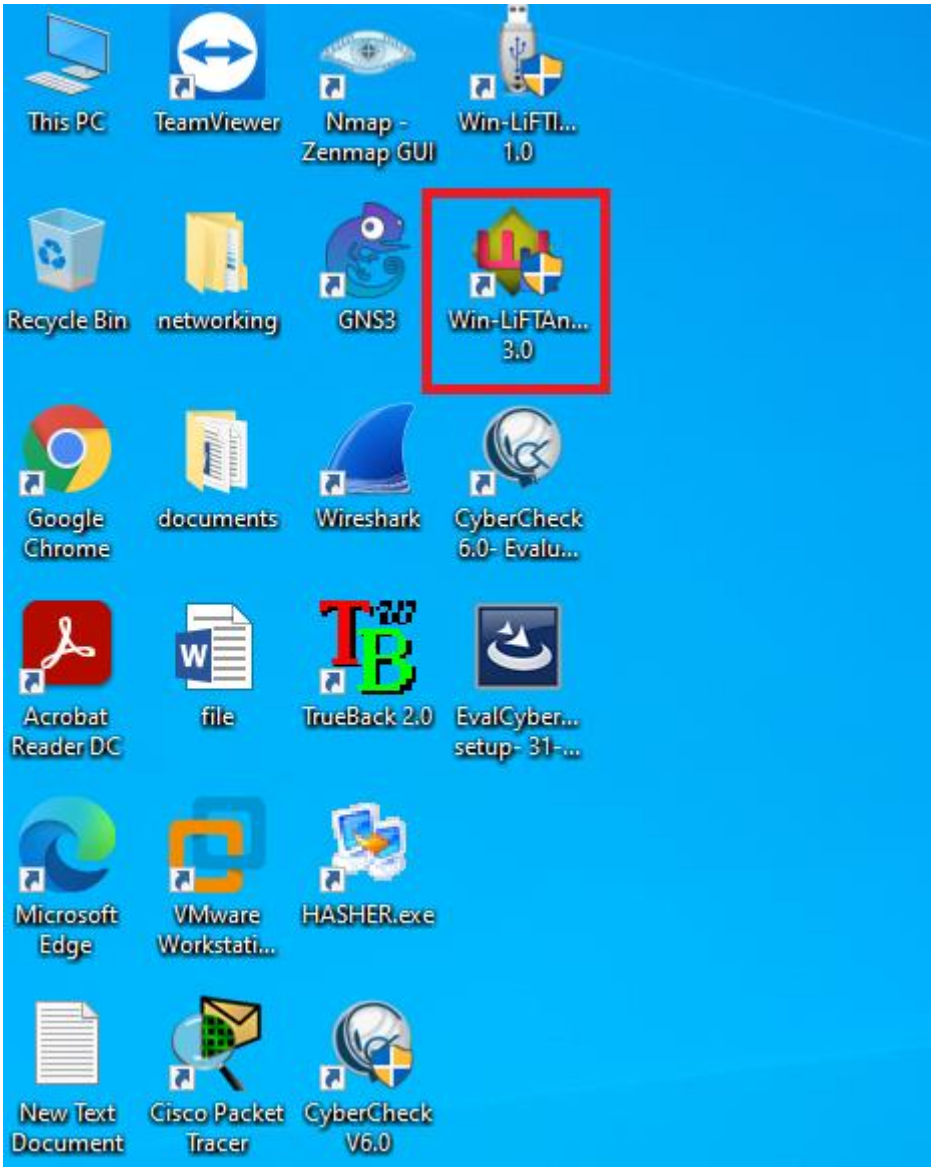

Figure 1: Open WinLiFT Analyzer Tool

Figure 2: Click File Tab

Figure 3: A New CaseFile

Step 3: Click on "…" to open a case file as shown in Figure 4. Select Win-LiFT .cfs option and press OK as shown in Figure 5.

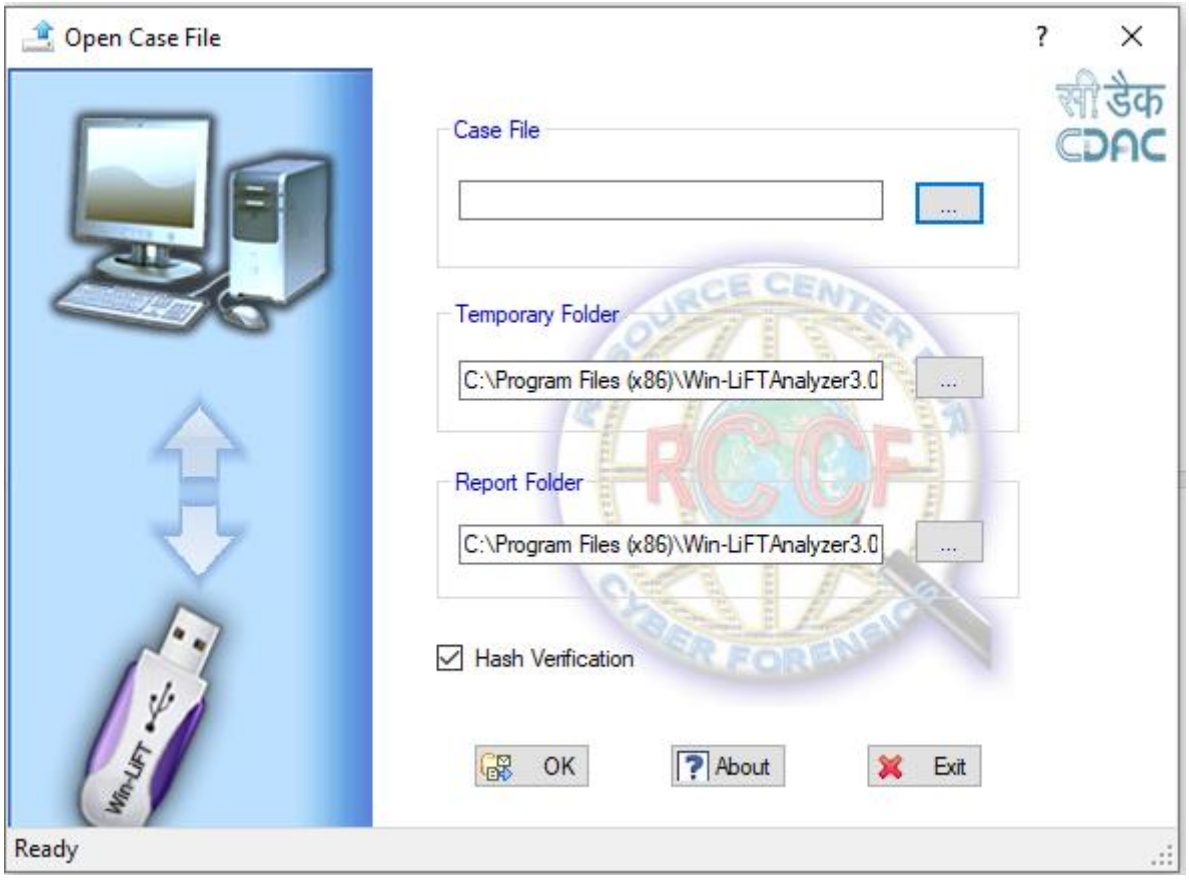

Figure 4: Open a new case

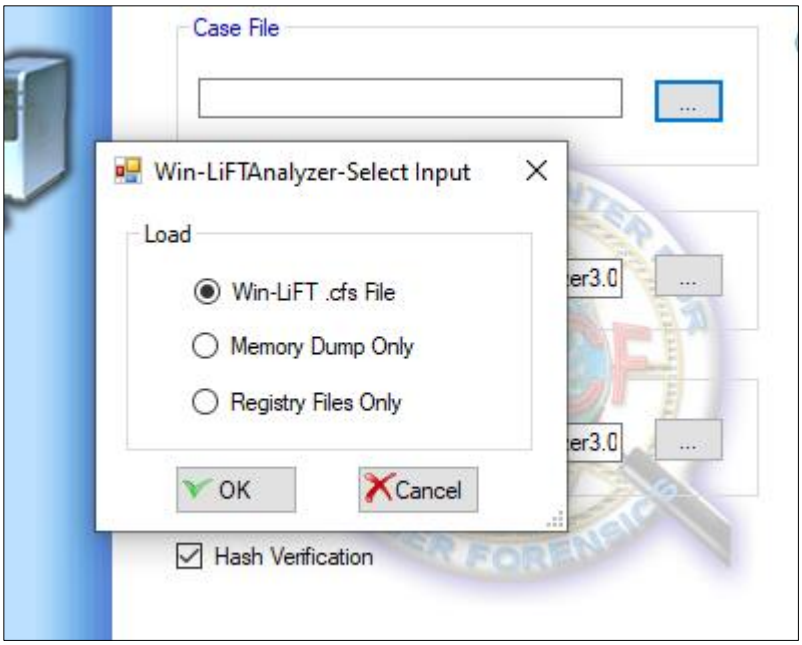

Figure 5: Open CFS File

Step 4: Open 135.cfs file from the USB (F:) as shown in Figure 6. This is the case file generated using WinLiFT ImagerBuilder tool. The path (F:\SHWETA SHARMA\135.cfs) will be displayed as shown in Figure 7. Press OK and then hash verification of the files will be performed as shown in Figure 8.

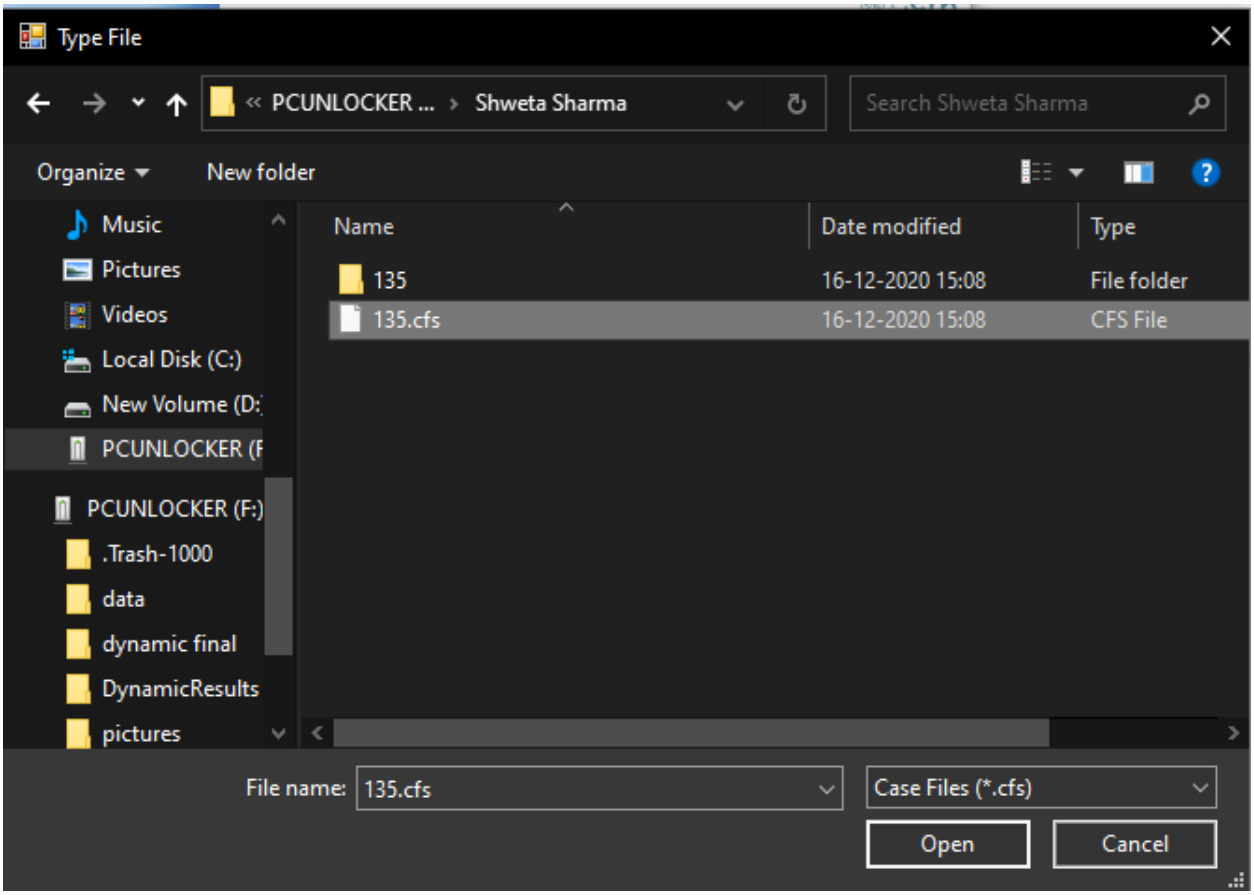

Figure 6: A CFS File

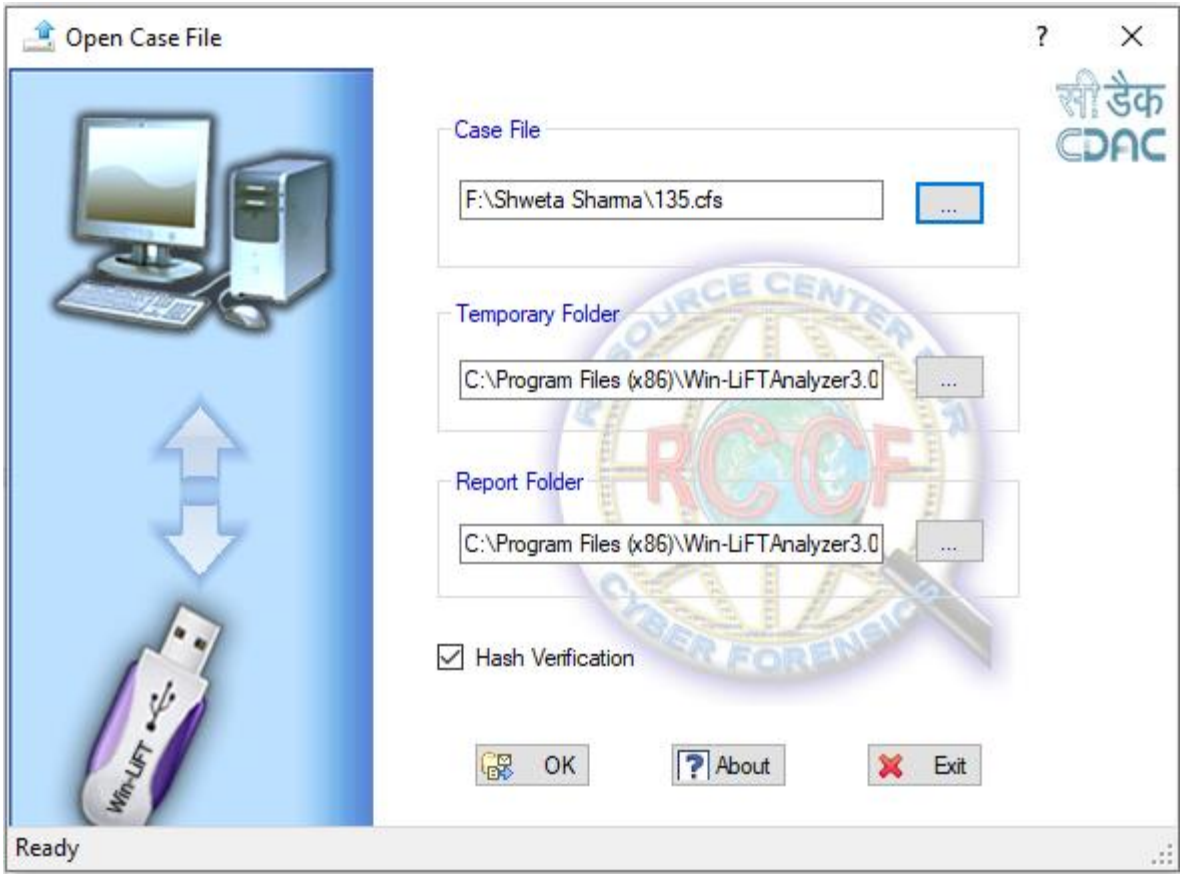

Figure 7: Path to CFS File

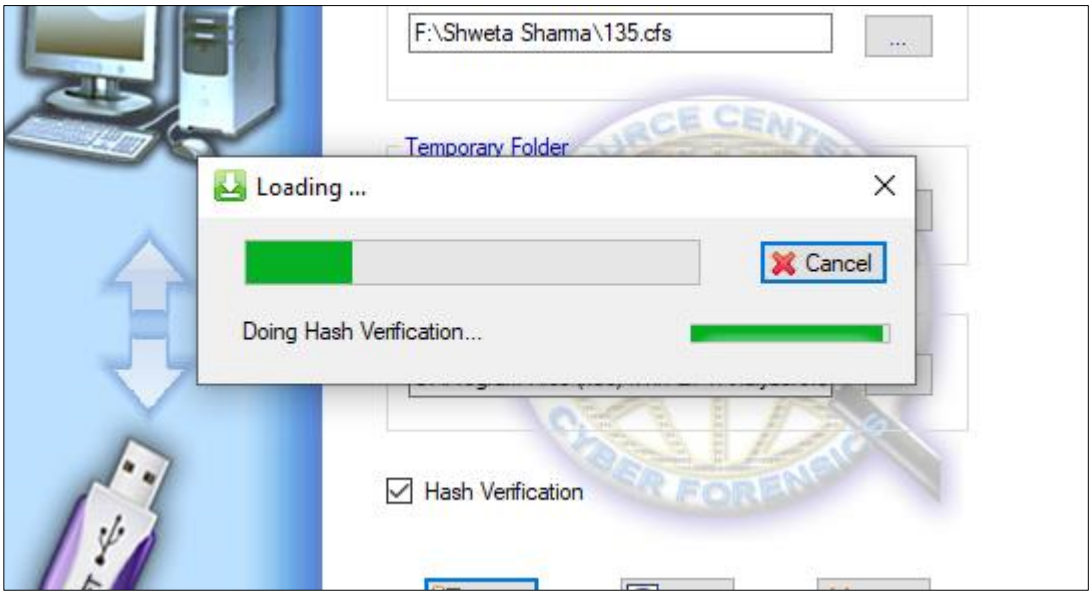

Figure 8: Hash Verification

Step 5: Three views, namely, Tree View on left side, List view in front, and summary view of selected row in the bottom will appear as shown in Figure 9. Click on system users to see the usrrs who have logged in the suspect machine including number of log on, last log on performed as shown in Figure 9.

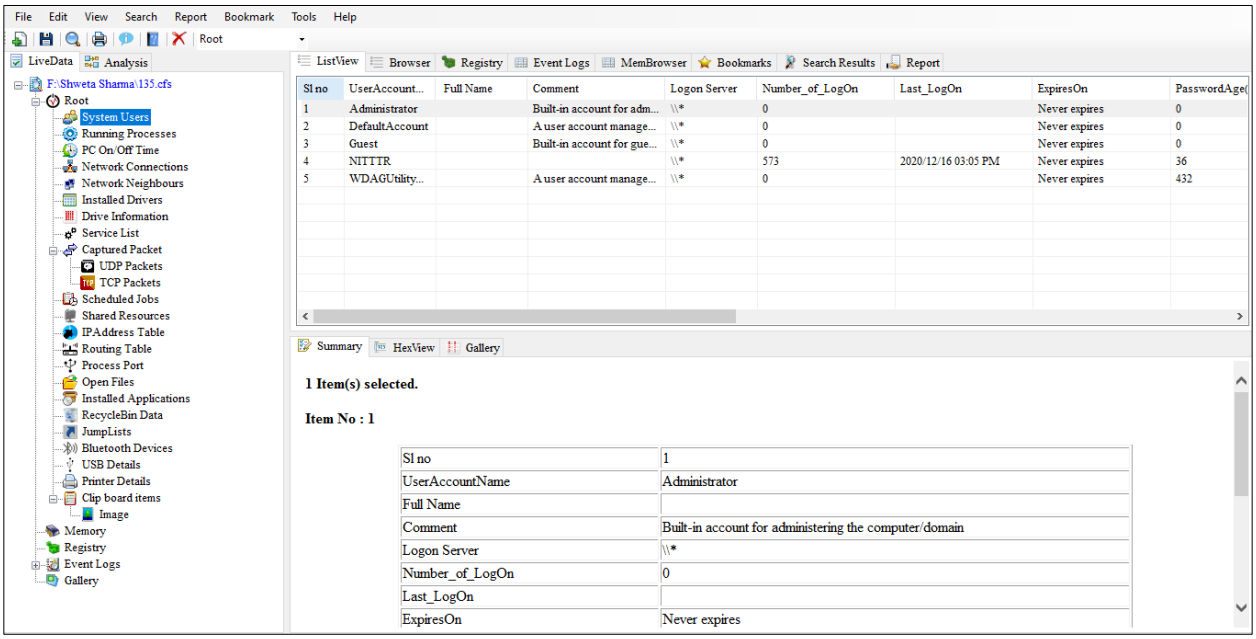

Figure 9: System Users

Step 6: After system users, the next is Running Processes (active program in execution mode). All running processes of suspect machine will be displayed in List view as shown in Figure 10.

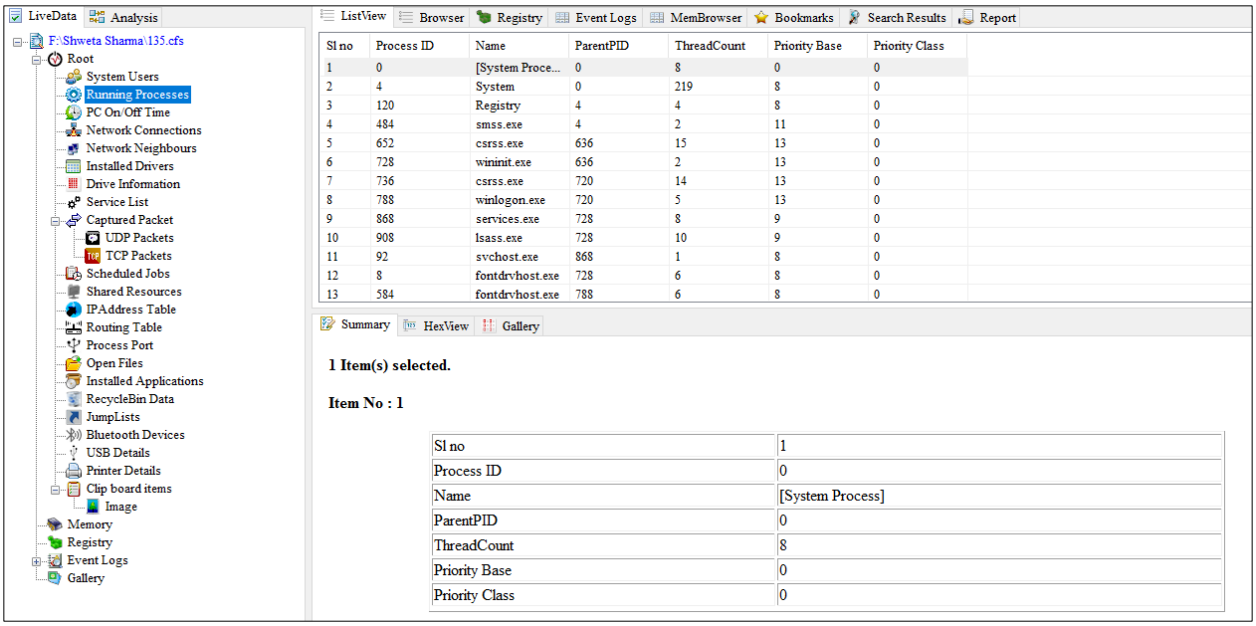

Figure 10: Running Processes

Step 7: Similarly after Running Processes, the PC ON/OFF time will be displayed in List view of the suspect machine as shown in Figure 11.

Step 8: After Running Processes, the Network connections of TCP and UDP protocol with source IP, destination IP, and STATE (LISTENINING, ESTABLISHED) will be displayed in List view of the suspect machine as shown in Figure 12.

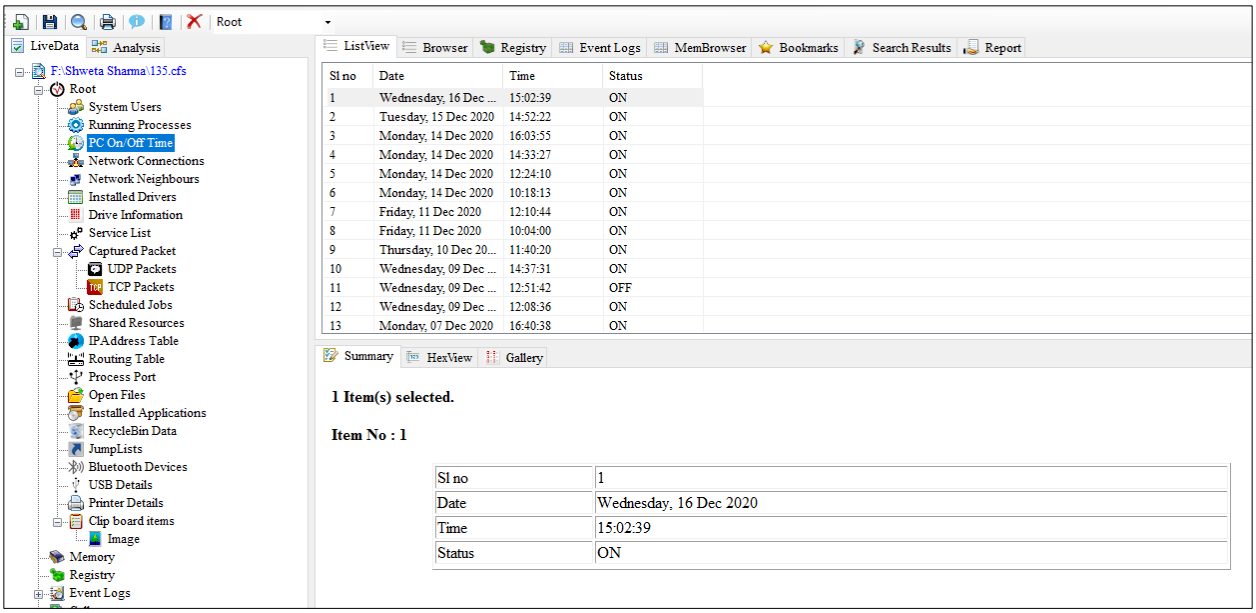

Figure 11: PC ON/OFF Time

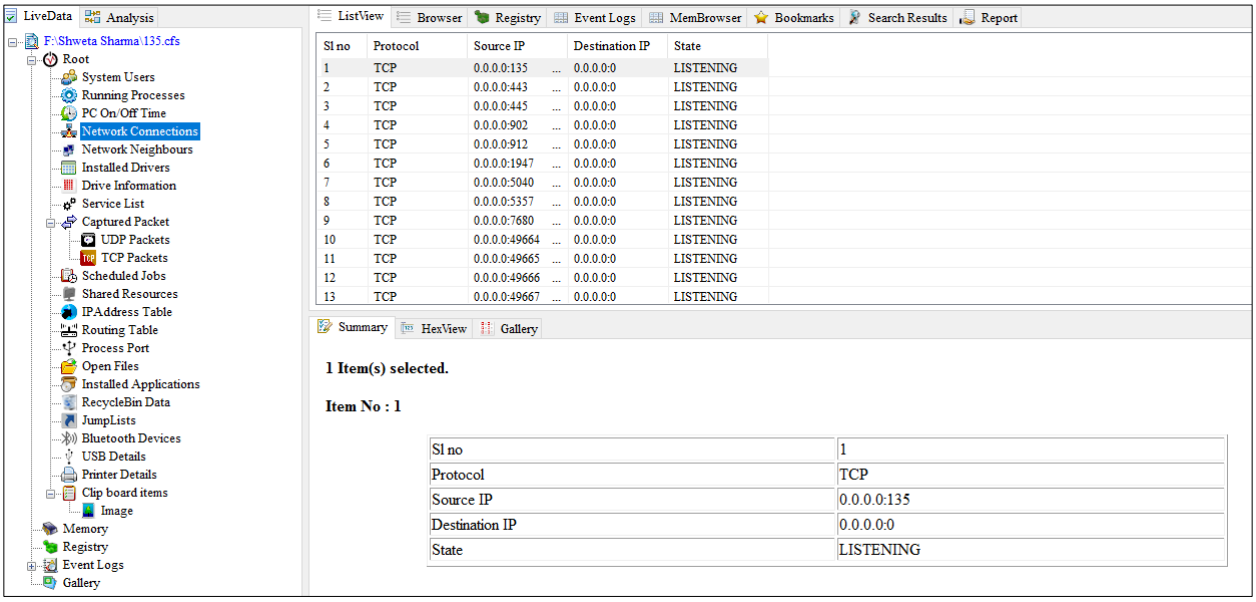

Figure 12: Network Connections

Step 9: After Network connections of TCP and UDP protocol, the Drive Information of local drives of the suspect machine and USB drive with Drive Name, Type, Volume Name, File

System, Free Space, and Total Space will be displayed in List view of the suspect machine as shown in Figure 13.

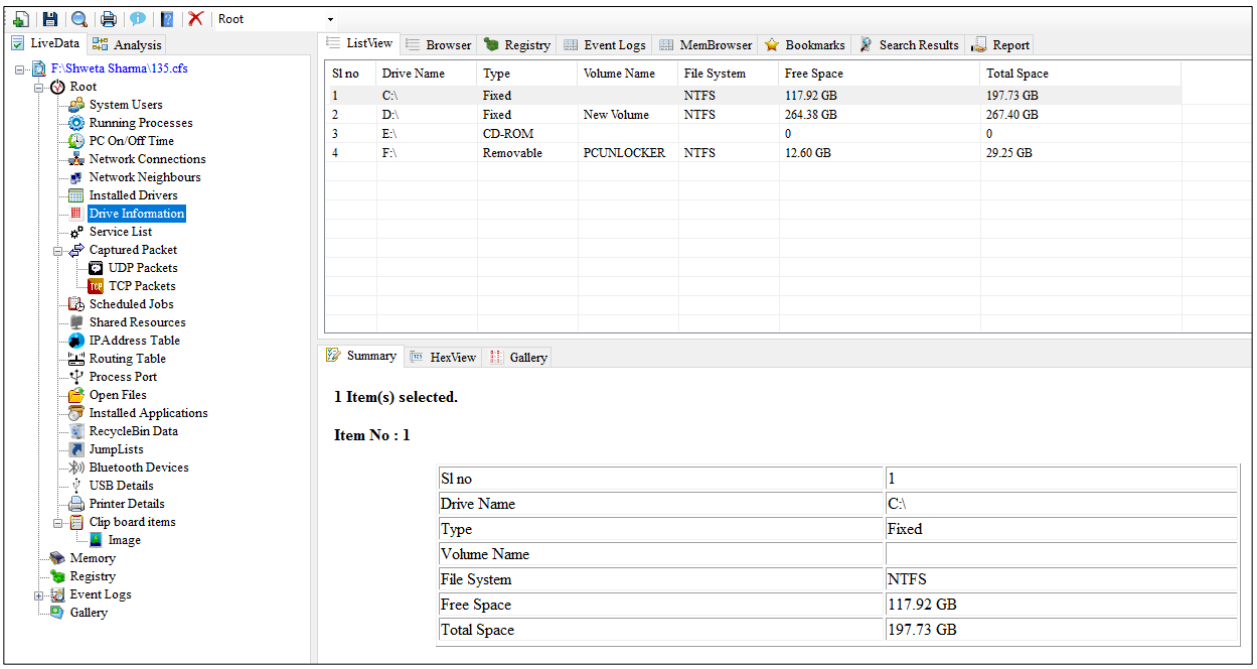

Figure 13: Drive Information

Step 10: On left hand side in the tree view, click Gallery to see the screenshots including Desktop wallpapers and icons of the suspect machine as shown in Figure 14. Right click on the image and select “Append to Report” to append the image to the report as shown in Figure 15.

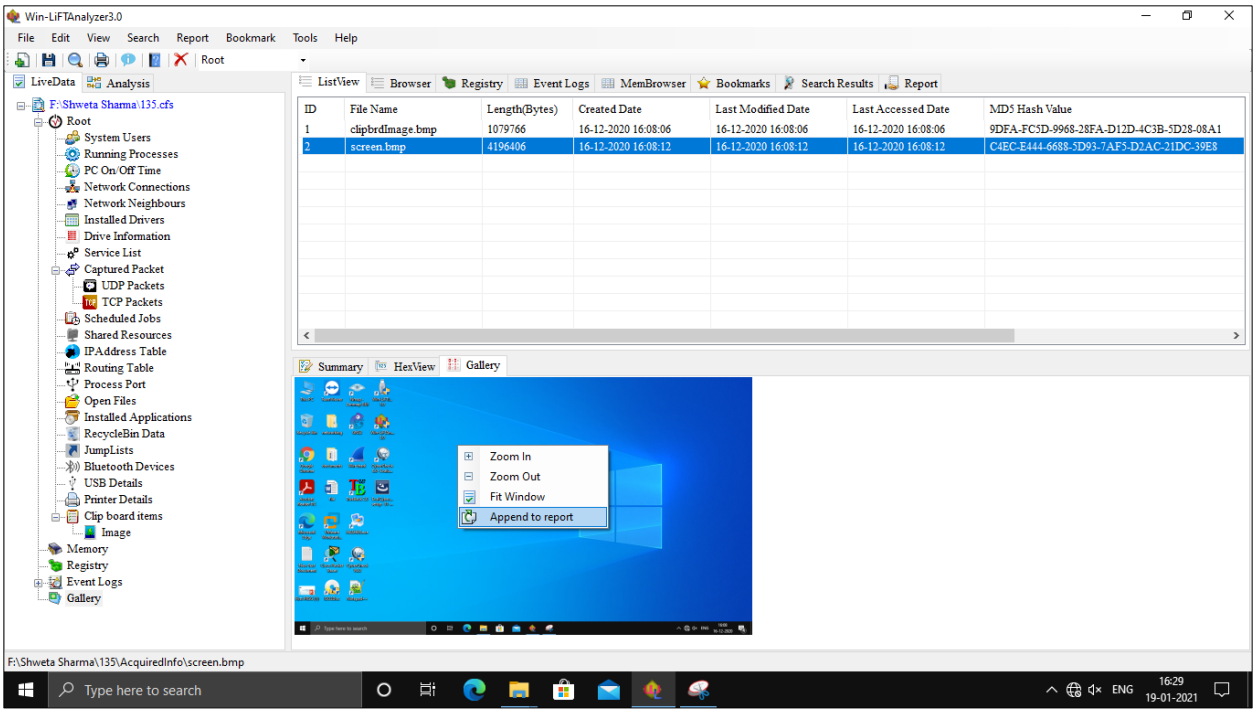

Figure 14: Gallery

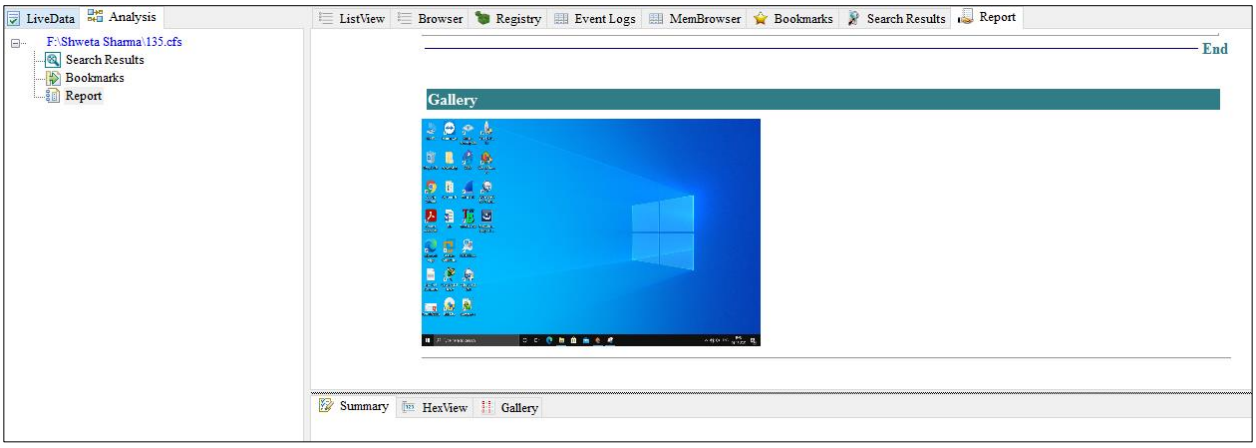

Figure 15: Report

Step 11: On left hand side in the tree view, click clipboard items to see the copied text and images of the suspect as shown in Figure 16. The copied image will be displayed in the bottom in summary view as shown in Figure 16.

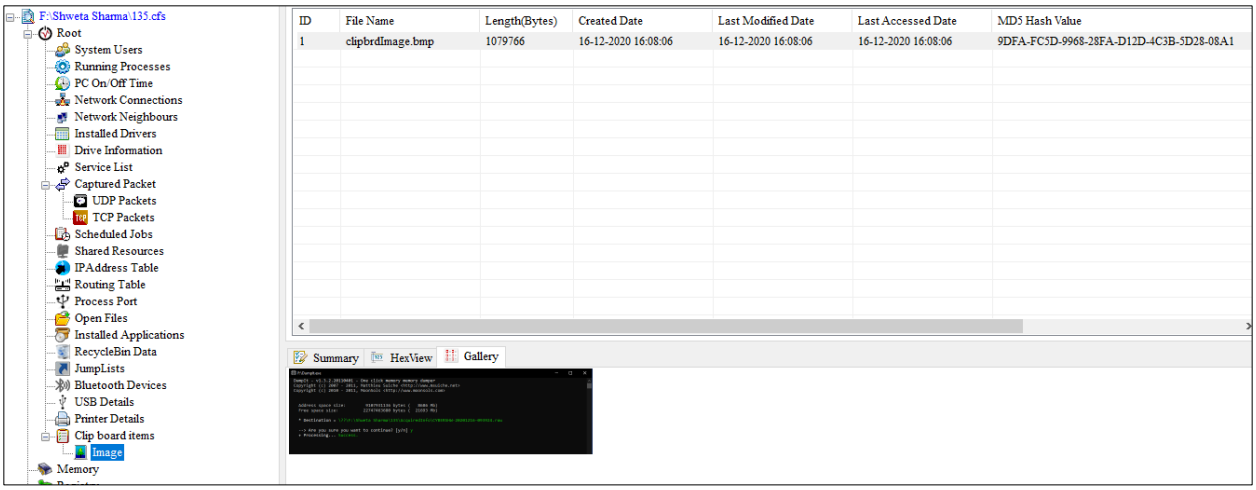

Figure 16: Clipboard Items

Step 12: To bookmark an item, go to Running processes in Tree View and select a process from List View. Right click on the selected process and select Bookmark item as shown in Figure 17. Provide a name and add comment to the selected process as shown in Figure 18.

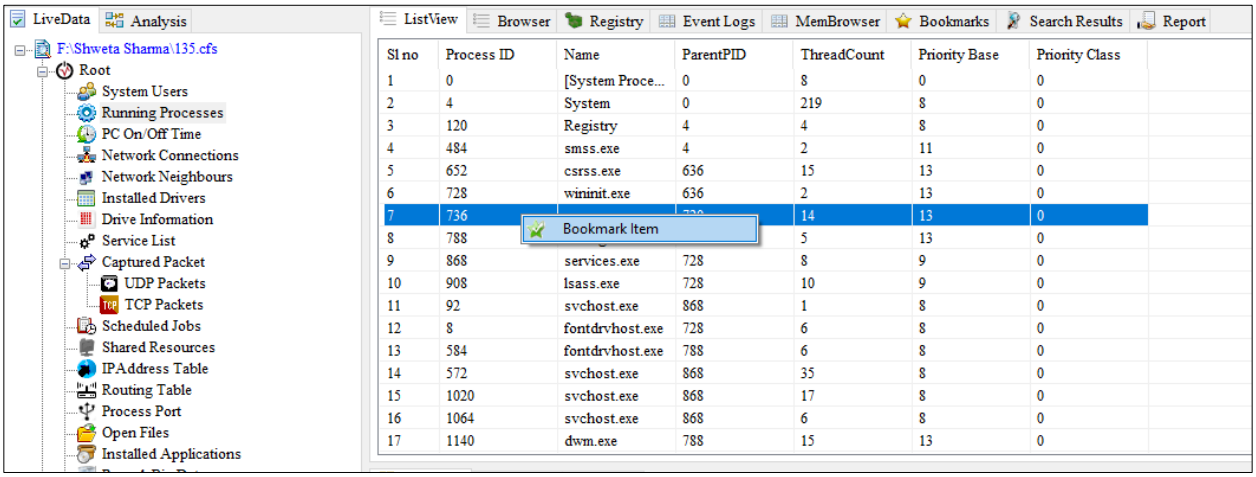

Figure 17: Bookmark

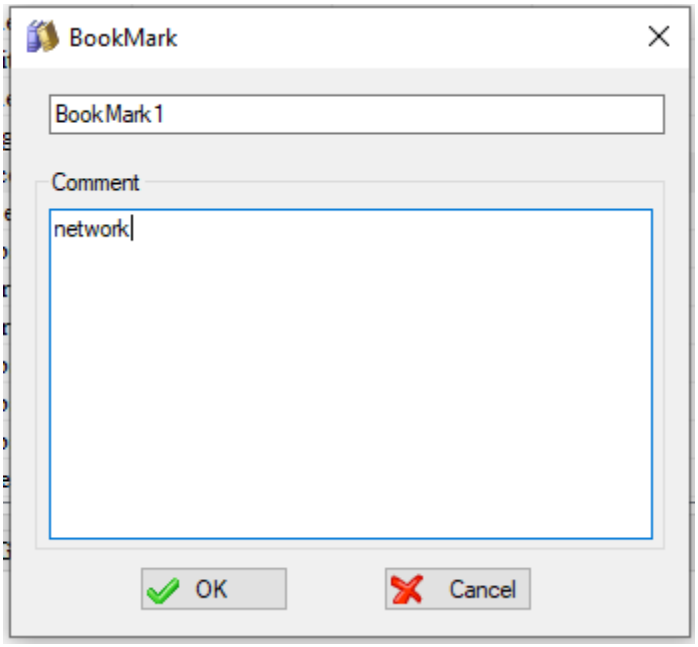

Figure 18: Name and Comment

Step 13: Go to Analysis on left hand side (Tree View) and select Bookmarks to see bookmarked items as shown in Figure 19. Right click on the bookmarked item and select "Append to Report" to append the item to the report as shown in Figure 20. Go to Report where the item has been appended to the report as shown in Figure 21.

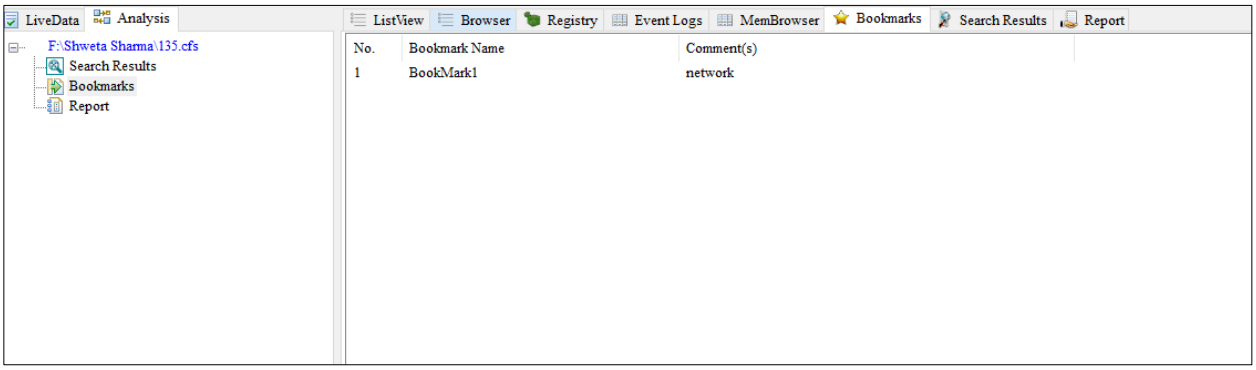

Figure 19: Bookmarked Items

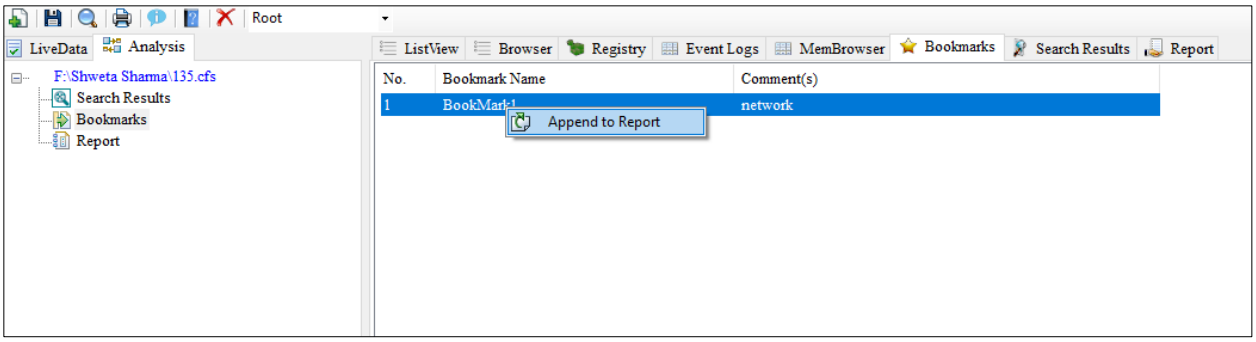

Figure 20: Append to Report

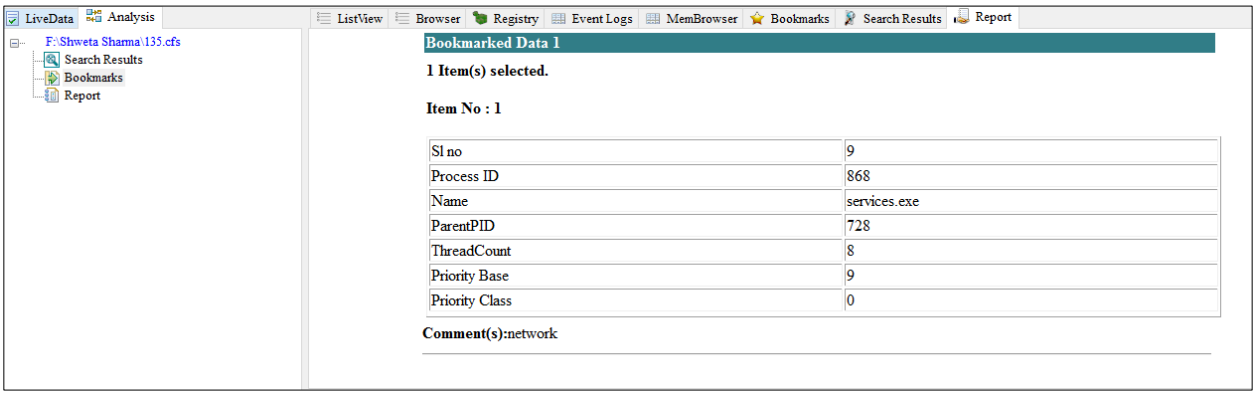

Figure 21: Item appended to the Report

Step 14: Go to Running processes on left hand side (Tree View) and click on search icon form the menu to perform search operation. Type a keyword (e.g., csrss) in the text box and click on search button as shown in Figure 22. The searched results of that keyword will be displayed as shown in Figure 23.

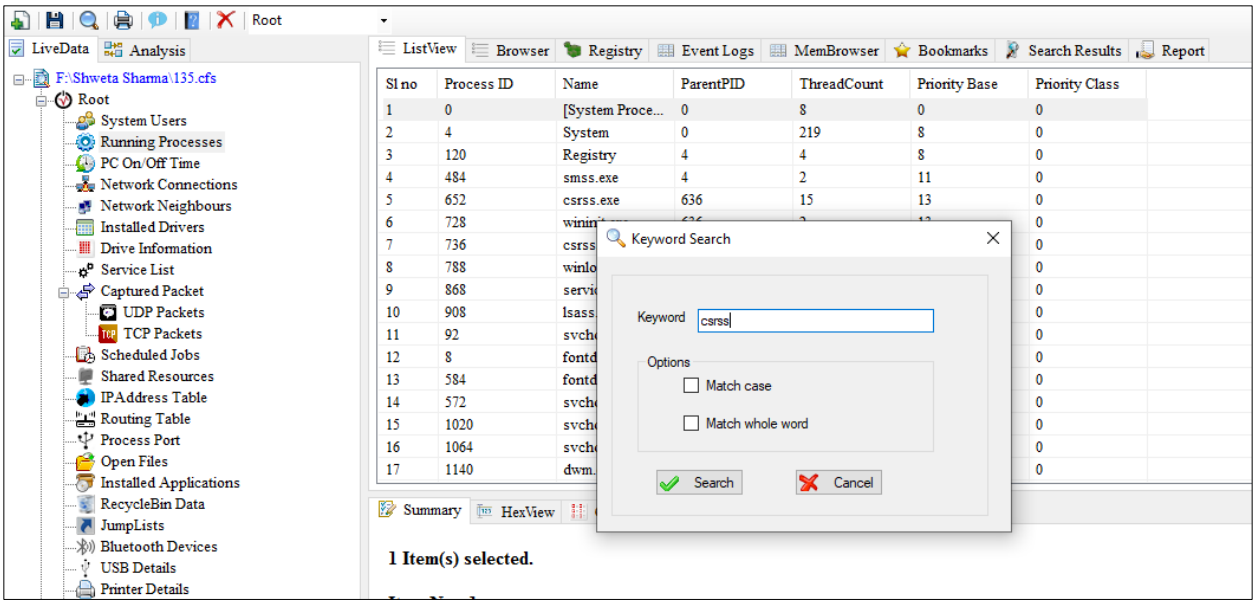

Figure 22: Keyword Search

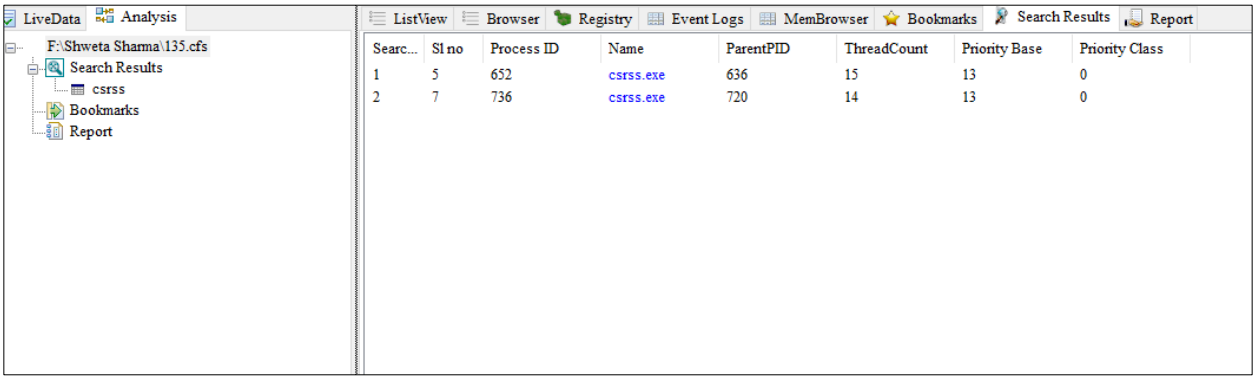

Figure 23: Searched Results

Step 15: Right click on the serached item and select “Append to Report” to append the item to the report as shown in Figure 24. Go to Report where the item has been appended to the report as shown in Figure 25.

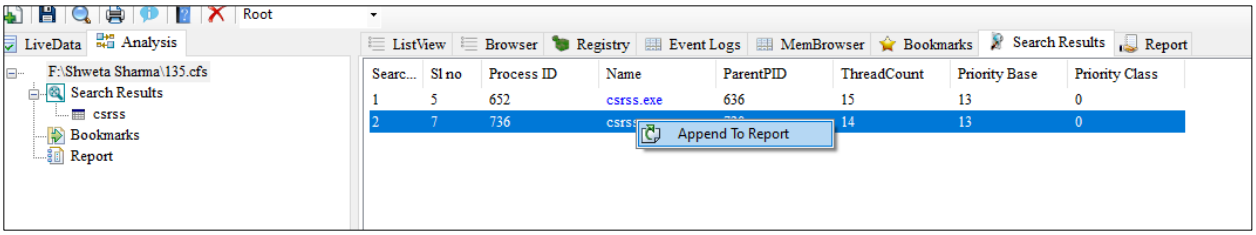

Figure 24: Append to Report

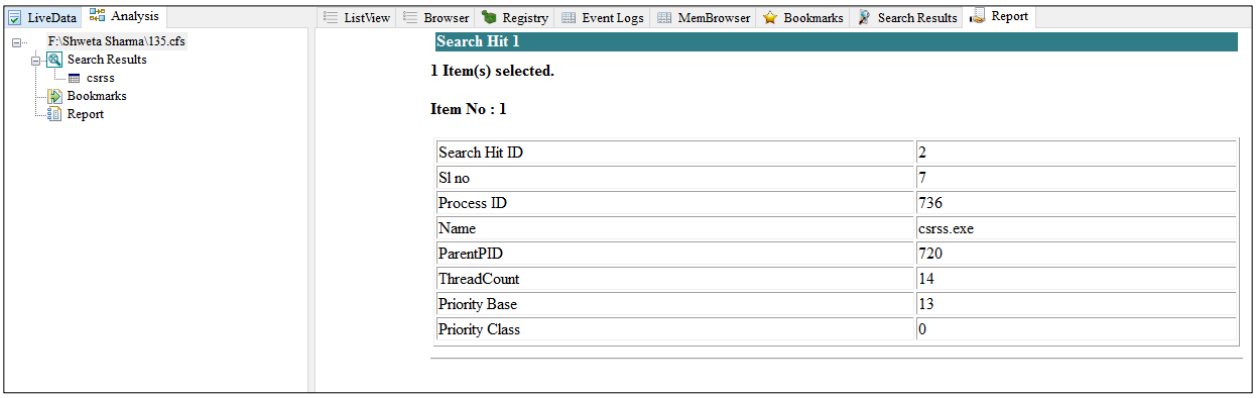

Figure 25: Final Report

By this way, the data acquires by the WinLiFT ImagerBuilder tool will be analyzed by the WinLiFT Analyzer tool.

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).