

#### 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

INTRODUCTION TO WINLIFT	2
TOOL: WINLIFT ANALYZER TOOL	3
HOW TO ANALYZE DATA WITH WinLiFT ANALYZER TOOL	4
REFERENCES	. 20

# **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

**<u>Step 1</u>**: Open WinLiFT Analyzer Tool after installation as shown in Figure 1.

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

This PC	FeamViewer	R Nmap - Zenmap GUI	Nin-Lifti		
Recycle Bin	networking	GNES	Win-LiFTAn 30		
Google Chrome	documents	Wireshark	CyberCheck 6.0-Evalu		
Acrobat Reader DC	file	TrueBack 2.0	EvalCyber setup: 31		
Microsoft Edge	VMware Workstati	HASHER.exe			
New Text Document	Cisco Packet Tracer	CyberCheck V6.0			

Figure 1: Open WinLiFT Analyzer Tool

🎨 Win-LiFTAnalyzer3.0			-	×
File Help				
🛃   🗭   🕎   🗙				
	Eigure 2	· Click Eile Tab		
	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0 File Help	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0 File Help New CaseFile Ctrl+N Open Saved CaseFile Ctrl+O	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0         File       Help         Yew CaseFile       Ctrl+N         Open Saved CaseFile       Ctrl+O         X       Exit       Alt+X	Figure 2	: Click File Tab		
<ul> <li>Win-LiFTAnalyzer3.0</li> <li>File Help</li> <li>✓ New CaseFile Ctrl+N</li> <li>➢ Open Saved CaseFile Ctrl+O</li> <li>✓ Exit Alt+X</li> </ul>	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0         File       Help         Y       New CaseFile       Ctrl+ N         Open Saved CaseFile       Ctrl+ O         X       Exit       Alt+ X	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0         File       Help         ♥       New CaseFile       Ctrl+N         ♥       Open Saved CaseFile       Ctrl+O         ★       Exit       Alt+X	Figure 2	: Click File Tab		
<ul> <li>Win-LiFTAnalyzer3.0</li> <li>File Help</li> <li>✓ New CaseFile Ctrl+N</li> <li>✓ Open Saved CaseFile Ctrl+O</li> <li>✓ Exit Alt+X</li> </ul>	Figure 2	: Click File Tab		
Win-LiFTAnalyzer3.0 File Help P New CaseFile Ctrl+N Open Saved CaseFile Ctrl+O K Exit Alt+X	Figure 2	: Click File Tab		
<ul> <li>Win-LiFTAnalyzer3.0</li> <li>File Help</li> <li>✓ New CaseFile Ctrl+N</li> <li>✓ Open Saved CaseFile Ctrl+O</li> <li>✓ Exit Alt+X</li> </ul>	Figure 2	: Click File Tab		
<ul> <li>Win-LiFTAnalyzer3.0</li> <li>File Help</li> <li>New CaseFile Ctrl+N</li> <li>Open Saved CaseFile Ctrl+O</li> <li>X Exit Alt+X</li> </ul>	Figure 2	: Click File Tab		
<ul> <li>Win-LiFTAnalyzer3.0</li> <li>File Help</li> <li>P New CaseFile Ctrl+N</li> <li>○ Open Saved CaseFile Ctrl+O</li> <li>★ Exit Alt+X</li> </ul>	Figure 2	: Click File Tab		
<ul> <li>Win-LiFTAnalyzer3.0</li> <li>File Help</li> <li>✓ New CaseFile Ctrl+N</li> <li>✓ Open Saved CaseFile Ctrl+O</li> <li>✓ Exit Alt+X</li> </ul>	Figure 2	: Click File Tab		

**<u>Step 3</u>**: 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

🖁 Win-LiFTAn	alyzer-Select Inpu	t X	
Load			42
Win-I	LiFT .cfs File	e	r3.0
	ory Dump Only		C TA
	stry Files Only		
-	-	e	r3.0
₩ ОК	Cancel		200
Hash V	/enfication	FORE	

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.

🔛 Type File		×
← → ∽ ↑ 🔤 « PCUNLOCKER → Shweta Sharma v 🖏	Search Shweta Sharm	م ه
Organize 👻 New folder		- 🔳 😲
Music ^ Name ^	Date modified	Туре
🔚 Pictures 🔤 135	16-12-2020 15:08	File folder
Videos 135.cfs	16-12-2020 15:08	CFS File
🏪 Local Disk (C:)		
👝 New Volume (D:		
PCUNLOCKER (F:)		
Trash-1000		
data		
dynamic final		
DynamicResults		
pictures V <		>
File name: 135.cfs	✓ Case Files (*.cfs)	~
	Open	Cancel .:

Figure 6: A CFS File



Figure 7: Path to CFS File

	F:\Shweta Sharma\13	35.cfs	
	Temporary Folder	X	Ĩ.
		X Cancel	
Doing	Hash Verification		
1	Hash Verification	R FOREMEN	
12	(Card)		

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.

File Edit View Search Report Bookmark Tools	ls Hel	p							
📲 😫 🔍 🚔 🐢 🕎 🗙 Root 🔹									
🔽 LiveData 🚟 Analysis	ListVie	w 🗏 Browser	🐚 Registry	💷 Event Logs 🔛 MemBro	wser 🙀 Bookn	narks 🔰 Search Results	I Report		
E- F:\Shweta Sharma\135.cfs	lno T	UserAccount	Full Name	Comment	Logon Server	Number_of_LogOn	Last_LogOn	ExpiresOn	PasswordAge(
B Root		Administrator		Built-in account for adm	//*	0		Never expires	0
2 System Users	1	DefaultAccount		A user account manage	//*	0		Never expires	0
C DC On CONTINUE 3	(	Guest		Built-in account for gue	//*	0		Never expires	0
Network Connections 4	1	NITTTR		-	//*	573	2020/12/16 03:05 PM	Never expires	36
Network Neighbourg	1	WDAGUtility		A user account manage	//*	0		Never expires	432
Installed Drivers									
Drive Information									
n <sup>o</sup> Service List									
Captured Packet									
UDP Packets									
TCP Packets									
- Cheduled Jobs									
Shared Resources <									>
IPAddress Table									
📇 Routing Table 😰	Summa	ny 💷 HexView	Gallery						
Process Port									
	Item(s	s) selected.							^
📅 Installed Applications									
	tem No	o:1							
		S1 no			1				
Printer Details		UserA	AccountName		Administrator				
Clip board items		Full N	lame						
Memory		Com	nent		Built-in account	for administering the co	omputer/domain		
b Registry		Logo	n Server		//*				
E-mail Event Logs     Gallery		Numb	er_of_LogOn	L	0				
		Last_	LogOn						
		Expire	esOn		Never expires				~

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.

Analysis	E List	iew 🗏 Browser	🐚 Registry 🔠	Event Logs	🖩 MemBrowser 🌖	🍹 Bookmarks 🛛 🗴	Search Results 🛛 🌡 Report
harma\135.cfs	S1 no	Process ID	Name	ParentPID	ThreadCount	Priority Base	Priority Class
	1	0	[System Proce	0	8	0	0
sers	2	4	System	0	219	8	0
rocesses	3	120	Registry	4	4	8	0
1 me	4	484	smss.exe	4	2	11	0
aighbours	5	652	csrss.exe	636	15	13	0
rivers	6	728	wininit.exe	636	2	13	0
mation	7	736	csrss.exe	720	14	13	0
t	8	788	winlogon.exe	720	5	13	0
Packet	9	868	services.exe	728	8	9	0
ackets	10	908	1sass.exe	728	10	9	0
ickets	11	92	svchost.exe	868	1	8	0
Jobs	12	8	fontdrvhost.exe	728	6	8	0
sources	13	584	fontdrvhost.exe	788	6	8	0
ort s Applications n Data	l Item Item ?	(s) selected. No : 1					
		S1 no				1	
i Devices ils						0	
i Devices ils itails		Proce	ess ID			v	
ı Devices ils tails l items		Proce	ess ID			[System Proc	cess]
Devices ils tails l items		Proce Name Parer	ess ID e ttPID			[System Proc	cess]
Devices ls tails items		Proce Name Parer Threa	ess ID e ttPID tdCount			[System Proc 0 8	cess]
Devices Is ails items		Proce Name Parer Threa Priori	ess ID e ttPID tdCount ty Base			0           [System Proc           0           8           0	:ess]

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.

**<u>Step 8</u>**: 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.

Data 👫 Analysis	🗏 List	View 🔚 Browser 🐚	Registry	Event Logs	III MemBrowser	🙀 Bookmarks	🔰 Search Results	I Report
Shweta Sharma\135.cfs	S1 no	Date	Time	Status				
Root	1	Wednesday, 16 Dec.	15:02:39	ON				
System Users	2	Tuesday 15 Dec 2020	14.52.22	ON				
Running Processes	3	Monday 14 Dec 2020	16:03:55	ON				
PC On/Off Time	4	Monday, 14 Dec 2020	14-33-27	ON				
Network Connections	5	Monday, 14 Dec 2020	12:24:10	ON				
Network Neighbours	6	Monday, 14 Dec 2020	10:18:13	ON				
Installed Drivers	7	Friday 11 Dec 2020	12:10:44	ON				
Barrian List	8	Friday, 11 Dec 2020	10:04:00	ON				
Contrared Backet	0	Thursday, 10 Dec 20	11:40:20	ON				
	10	Wednesday, 10 Dec 20.	14:37:31	ON				
TCP Packets	10	Wednesday, 09 Dec	12:51:42	OFF				
Scheduled Jobs	12	Wednesday, 09 Dec	12:08:36	ON				
Shared Resources	13	Monday: 07 Dec 2020	16:40:38	ON				
IPAddress Table		Monday, 07 Dec 2020	10.40.50	011				
Routing Table	🔯 Sum	mary 🛅 HexView 🚦	Gallery					
· Process Port			_					
🔗 Open Files	1 Iter	m(s) selected.						
👦 Installed Applications		~						
	Item	No:1						
券》)Bluetooth Devices		C1						
🖞 USB Details		SI no		1				
		Date		Wednes	day, 16 Dec 202	0		
E 🗂 or e en		T.		15.00.20	)			
Cip board items		1 me		111112 19				



Coldia NII Allalysis	i List	hew 😑 Browser	🐞 Registry	Event Logs 🛛 🔠	MemBrowser	🙀 Bookmarks	s 🕺 Search Results 🛛 딇 Repor	ıt
F:\Shweta Sharma\135.cfs	S1 no	Protocol	Source IP	Destination IP	State			
- 🛞 Root	1	TCP	0.0.0.135	 0.0.0.0:0	LISTENING			
System Users	2	TCP	0.0.0.0:443	 0.0.0.0:0	LISTENING			
Running Processes	3	TCP	0.0.0.0:445	 0.0.0.0:0	LISTENING			
PC On/Off Time	4	TCP	0.0.0.0:902	 0.0.0.0:0	LISTENING			
Network Veighbourg	5	TCP	0.0.0.912	 0.0.0.0:0	LISTENING			
Installed Drivers	6	TCP	0.0.0.0:1947	 0.0.0.0:0	LISTENING			
Drive Information	7	TCP	0.0.0.0:5040	 0.0.0.0:0	LISTENING			
<sup>p</sup> Service List	8	TCP	0.0.0.0:5357	 0.0.0.0:0	LISTENING			
Captured Packet	9	TCP	0.0.0.7680	 0.0.0.0:0	LISTENING			
UDP Packets	10	TCP	0.0.0.0:49664	 0.0.0.0:0	LISTENING			
TCP Packets	11	TCP	0.0.0.0:49665	 0.0.0.0:0	LISTENING			
Scheduled Jobs	12	TCP	0.0.0.0:49666	 0.0.0.0:0	LISTENING			
💷 👮 Shared Resources	13	TCP	0.0.0.0:49667	 0.0.0.0:0	LISTENING			
🗊 IPAddress Table								
Routing Table	💱 Sum	mary 🔤 HexView	v Gallery					
Process Port								
🚰 Open Files	1 Iter	n(s) selected.						
RecycleBin Data	Item	No : 1						
M Direct att Davisor								
USB Details		S1 no					1	
Printer Datails		Droto	a col				TCD	
Clin board items		FIOR					ICF	
Image		Source	ce IP				0.0.0.0:135	
Memory		Desti	nation IP				0.0.0.0	
hegistry		State					LISTENING	
and the second s		State					LIGILIANO	

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.

👿 LiveData 📑 Analysis	🗉 List	View 🔚 Browse	r 🐚 Registry	🔜 Event Logs 🔠	MemBrowser	🙀 Bookmarks 🏼 🎉 Sea	rch Results 👃 Report	
F: Shweta Shama 135.cfs      System Users      System Users      PC On/Off Time      Network Connections      Network Connections      Network Neighbours      Installed Drivers      Drive Information      o <sup>®</sup> Service List      Captured Packets      DUP P	St no 1 2 3 4 4 5 5 5 Sun 1 1 1 1 1 1 1 1 2 3 3 4 4 1 1 1 2 3 3 4 4 1 1 1 1 1 1 1 1 1 1 1 1 1	Drive Name C:\ D:\ E:\ F:\ F:\ many (m HexVie m(s) selected.	Type Fixed Fixed CD-ROM Removable	Volume Name New Volume PCUNLOCKER	File System NTFS NTFS NTFS	Free Space 117.92 GB 264.38 GB 0 12.60 GB	Total Space 197.73 GB 267.40 GB 0 29.25 GB	
RecycleBin Data JumpLists Bluetooth Devices Clip Doard items Image Memory Registry Gallery	Item	No:1 SIn Driv Typ Voh File Free Totz	o e Name e me Name System : Space il Space			1 C Fi N 11 15	A xed TFS 17.92 GB 97.73 GB	

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.

win-LiFiAnalyzer5.0							- 0
ile Edit View Search Report Bookman	k Tools H	lelp					
🗋   💾   🔍   🚔   🐢   🔟   🗡   Root	-						
LiveData 👫 Analysis	💷 List\	/iew 🔚 Browser 🐚 I	Registry 📰 Event	Logs 🔠 MemBrowser	🙀 Bookmarks 🏼  Searc	h Results 🛛 👃 Report	
	ID	File Name	Length(Bytes)	Created Date	Last Modified Date	Last Accessed Date	MD5 Hash Value
Root	1	clipbrdImage bmp	1079766	16-12-2020 16:08:06	16-12-2020 16:08:06	16-12-2020 16:08:06	9DFA-FC5D-9968-28FA-D12D-4C3B-5D28-08A1
System Users	2	screen.bmp	4196406	16-12-2020 16:08:12	16-12-2020 16:08:12	16-12-2020 16:08:12	C4EC-E444-6688-5D93-7AF5-D2AC-21DC-39E8
Running Processes							
Network Connections							
Network Neighbours							
- Installed Drivers							
	_						
- o <sup>p</sup> Service List							
- P Captured Packet							
CDP Packets							
Scheduled John							
Shared Resources	<						
- 🗿 IPAddress Table							
	📝 Sum	mary ២ HexView 📗	Gallery				
Process Port	2 😥	se 🔥					
Open Files	Ref: Institut	And the second s					
RecycleBin Data	Acres in another	, 🐔 🌨					
JumpLists	<b>•</b> •	4 0					
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Straight Annual	· manage and resolution	± Zoom In				
	<b>P</b> a	T. 🖸	<ul> <li>Zoom Out</li> </ul>				
	Doobas Ko Konoviti	Salad 15 Salipan.	Fit Window				
E- Clip board items	R 🖸	ي ا	Append to report	nt			
image Image	Advented National Dige Madvande	and and an					
The Registry	the for						
Event Logs	Stemant Rear						
Gallery	autoria antes	All and a second se					
-							
	P Type he	re to search O 12	<u>• = ii = • •</u>	^ Q	p me with the second se		
Shunda Sharma) 125) Accuired lefa) screen bran							16:20
shweta Sharma\135\AcquiredInfo\screen.bmp	_				-		10/21 -
inweta Sharma\135\AcquiredInfo\screen.bmp		o ≓	💽 📮 🧯	i 📄 🍭 🖉			$\wedge \bigoplus \triangleleft \forall \times ENG \xrightarrow{10-29} \square$

LiveData 🗮 Analysis	🗄 ListView 🗏 Browser 🐌 Registry 💷 Event Logs 💷 MemBrowser 😭 Bookmarks 🦹 Search Results 🎣 Report	
↓ LiveData     №5     Analysis       □-     F:Shweta Sharma 135.cfs       ●     Bookmarks       ●     Bookmarks       ●     Report	E ListView E Browser Registry E Event Logs MemBrowser Report	End
	Summary Review II 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.

:\Shweta Sharma\135.cfs	ID	File Name	Length(Bytes)	Created Date	Last Modified Date	Last Accessed Date	MD5 Hash Value
Root	1	clipbrdImage.bmp	1079766	16-12-2020 16:08:06	16-12-2020 16:08:06	16-12-2020 16:08:06	9DFA-FC5D-9968-28FA-D12D-4C3B-5D28-08A
🚰 System Users		1					
- O Running Processes							
- 🕒 PC On/Off Time							
- 💑 Network Connections							
🛃 Network Neighbours							
Installed Drivers							
Drive Information							
✿ <sup>P</sup> Service List							
– 🔄 Captured Packet							
UDP Packets							
TCP Packets							
Scheduled Jobs							
Shared Resources							
- 🗿 IPAddress Table							
Routing Table							
Process Port							
🛁 Open Files							
- TInstalled Applications	<						
	Role at		College				
JumpLists	📝 Su	mmary 🛄 HexView 🚹	Gallery				
	El M.Compton Demp04 - v3.3. Copyright (c)	2.20130400 - Des tlick manary memory damper 2007 - 2011, Natthies Saiche cittp://www.assiche.net					
	Empyright (c)	2000 - 2011, Montholic (HTTp://www.weoncolic.com)					
Printer Details	Tree space of	5 6124) 9107911156 97541 ( 3600 80) LLa: 22341463000 9ytes ( 20033 80)					
oup courd nexts							

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.

↓ LiveData  Analysis	🗏 List\	iew 🗏 Browser	🐚 Registry 🔠	Event Logs	MemBrowser 🖕	Bookmarks 🎉	Search Results 👃 Report
	S1 no	Process ID	Name	ParentPID	ThreadCount	Priority Base	Priority Class
E Soot	1	0	[System Proce	0	8	0	0
System Users	2	4	System	0	219	8	0
Running Processes	3	120	Registry	4	4	8	0
Network Connections	4	484	smss.exe	4	2	11	0
Network Neighbours	5	652	csrss.exe	636	15	13	0
Installed Drivers	6	728	wininit.exe	636	2	13	0
Drive Information	7	736		720	14	13	0
Bervice List	8	788	Bookmark Item		5	13	0
Captured Packet	9	868	services.exe	728	8	9	0
UDP Packets	10	908	lsass.exe	728	10	9	0
TCP Packets	11	92	svchost.exe	868	1	8	0
Scheduled Jobs	12	8	fontdrvhost.exe	728	6	8	0
- E Shared Resources	13	584	fontdrvhost.exe	788	6	8	0
IPAddress Table	14	572	svchost.exe	868	35	8	0
Routing Table	15	1020	svchost.exe	868	17	8	0
Process Port	16	1064	svchost.exe	868	6	8	0
Upen Files	17	1140	dwm.exe	788	15	13	0
mistalied Applications							

Figure 17: Bookmark

🗊 BookMark	×
BookMark1	
Comment	
network	
r	
r ,	
, ,	
>	
-	
✓ ОК	🔀 Cancel

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.

LiveData	💷 ListVie	w 🗏 Browser	🐌 Registry 🔠 Event	Logs 🛄 MemBrowser	🙀 Bookmarks	🔰 Search Results	I Report
	No. E	ookmark Name		Comment(s)			
- Search Results	1 E	ookMark1		network			
Report							



🖺   💾   🔍   🖨   🕫   👔   🗡   Root	•	
LiveData 👫 Analysis	📒 ListView 🗮 Browser 🝗 Registry 📖 Ever	nt Logs 💷 MemBrowser 🙀 Bookmarks 🦹 Search Results 🚚 Repor
	No. Bookmark Name	Comment(s)
Image: Search Results         Image: Search Results <td< th=""><th>1 BookMart+1</th><th>network</th></td<>	1 BookMart+1	network
	Figure 20: Append to	o Report
ItveData 🚟 Analysis	Figure 20: Append to	D Report
IveData Analysis F:Shweta Shama 135.cfs Search Results Bookmarks Report	Figure 20: Append to	D Report
LiveData Analysis - F:Shweta Shama 135.cfs Soearch Results Bookmarks I Report	Figure 20: Append to ListView Browser Registry Event Logs MemBrow Bookmarked Data 1 1 Item(s) selected. Item No : 1	o Report vser 😭 Bookmarks  Search Results 🖓 Report
LiveData Results F:Shweta Sharma'135.cfs Sockarks Report	Figure 20: Append to	o Report
LiveData Shama\135.cfs - F:Shweta Shama\135.cfs - & Search Results - & Bookmarks - & Report	Figure 20: Append to	D Report
LiveData Analysis - F:Shweta Shama 135.cfs - G Search Results - Bookmarks - Report	Figure 20: Append to	D Report
LiveData Analysis - F:Shweta Shama 135.cfs - Search Results - Bookmarks - Report	Figure 20: Append to	Po Report  vser 🖈 Bookmarks 👂 Search Results 🔊 Report  9  868 services.exe 728
LiveData Sanalysis	Figure 20: Append to	P Report New Report Search Results Report 9 868 services.exe 728 8
LiveData 25 Analysis - F:Shweta Shama 135 cfs Search Results Bookmarks Report	Figure 20: Append to	P Report Ner Report Search Results Report 9 868 services.exe 728 8 9 9

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.

						1.84	
LiveData 👫 Analysis	💷 List	View 🗮 Browser	🐚 Registry 🔠	Event Logs	🔠 MemBrowser 🍏	🏹 Bookmarks 🛛 🦹	Search Results 🛛 👃 Report
	S1 no	Process ID	Name	ParentPID	ThreadCount	Priority Base	Priority Class
⊡ · 🚱 Root	1	0	[System Proce	0	8	0	0
System Users	2	4	System	0	219	8	0
Running Processes	3	120	Registry	4	4	8	0
Network Connections	4	484	smss.exe	4	2	11	0
Network Neighbours	5	652	csrss.exe	636	15	13	0
Installed Drivers	6	728	winin'	121	2	12	0
Drive Information	7	736	csrss 🤍 Keywo	ord Search		×	0
Bervice List	8	788	winlo				0
🖃 🚽 Captured Packet	9	868	servic				0
UDP Packets	10	908	Isass Keywo	ord cereel			0
TCP Packets	11	92	svch	Caraa			0
- 🔂 Scheduled Jobs	12	8	fontd Opti	ons			0
	13	584	fontd	Match case			0
	14	572	svch				0
Routing Table	15	1020	svche	Match whole	word		0
	16	1064	svch				0
Upen Files	17	1140	dwm.	A Caarab	V Canad		0
RecycleBin Data	82	-	×	Search	A Cancel		
	📝 Sum	mary 🔤 HexView					
	l Iter	n(s) selected.					
	-						



🖌 LiveData 👫 Analysis	🗏 ListV	iew 🚞	Browser 🐚 Reg	gistry 🛄 Event I	.ogs 🔛 MemBro	owser 🙀 Bookm	arks 🔰 Search I	Results 👃 Report
E F:\Shweta Sharma\135.cfs	Searc	Sl no	Process ID	Name	ParentPID	ThreadCount	Priority Base	Priority Class
E Search Results	1	5	652	csrss.exe	636	15	13	0
Bookmarks	2	7	736	csrss.exe	720	14	13	0
Report								

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.

] 💾 🔍 🚔 🕫 🔢 🔭 Root	•				
LiveData Analysis	🔚 ListView 🗮 Browser 🐚	Registry 🔛 Event Logs 🔜 Men	nBrowser 🙀 Book	marks 🎉 Search	h Results  👃 Repo
F:\Shweta Sharma\135.cfs	Searc SI no Process ID	Name ParentPID	ThreadCount	Priority Base	Priority Class
Search Results	1 5 652	csrss.exe 636	15	13	0
Bookmarks	2 7 736	Append To Report	14	13	0
	-				
	-				
LiveData	듣 ListView 듣 Browser 🍗 Registry 🖷	Event Lozs 🔛 MemBrowser 🩀 Bool	kmarks 👂 Search Res	ults 💊 Report	
LiveData 😽 Analysis - F:\Shweta Sharma\135.cfs	E ListView E Browser D Registry Search Hit 1	🛛 Event Logs 🔛 MemBrowser 🙀 Bool	kmarks     Search Res	sults 👃 Report	
LiveData 🚟 Analysis F:Shweta Sharma \135.cfs	E ListView E Browser Search Hit 1	🖩 Event Logs 🔠 MemBrowser 🙀 Bool	kmarks 👔 Search Res	aults 👃 Report	
LiveData Ranalysis → PiShweta Sharma 135.cfs → Search Results → Bookmarks → Report	E ListView E Browser D Registry Search Hit 1 Search Hit 1 I Item(s) selected. Item No : 1	🛿 Event Logs 🔛 MemBrowser 🙀 Bool	kmarks 🕺 Search Res	nults 🎝 Report	
LiveData Analysis F\Shweta Sharma 135.cfs Search Results Bookmarks Report	E ListView E Browser Search Hit 1 Search Hit 1 I Item (s) selected. Item No : 1 Search Hit ID	🛿 Event Logs 🔛 MemBrowser 🙀 Bool	kmarks 🖉 Search Res	ults 👃 Report	
LiveData 2 Analysis F:Shweta Sharma 135.cfs Search Results E csrss Bookmarks Report	E ListView E Browser Search Hit 1 Search Hit 1 I Item(s) selected. Item No : 1 Search Hit ID Sl no	🛿 Event Logs 🔛 MemBrowser 🙀 Bool	kmarks 🖉 Search Res	aults 👃 Report	
LiveData 2: Analysis F\Shweta Sharma 135.cfs Results Bookmarks Report	E ListView E Browser Registry Search Hit 1 I Item(s) selected. Item No : 1 Search Hit ID SI no Process ID	🛿 Event Logs 🔛 MemBrowser 🙀 Bool	kmarks 🖉 Search Res	nults 🎝 Report	
LiveData 2 Analysis F\Shweta Sharma 135.cfs Search Results Bookmarks Report	E ListView E Browser Registry Search Hit 1 I Item(s) selected. Item No : 1 Search Hit ID SI no Process ID Name	🖩 Event Logs 🔛 MemBrowser 🤺 Bool	kmarks 🖉 Search Res	aults 🚽 Report	
LiveData 2. Analysis F:Shweta Sharma\135.cfs Search Results Composition of the search of the sear	E ListView E Browser Registry Search Hit 1 I Item(s) selected. Item No : 1 Search Hit ID SI no Process ID Name ParentPID	🖩 Event Logs 🔛 MemBrowser 🦹 Bool	smarks P Search Res	aults 👃 Report	
LiveData Analysis F\Shweta Shama\135.cfs Search Results Bookmarks Report	E ListView E Browser Registry Search Hit 1 I Item(s) selected. Item No : 1 Search Hit ID SI no Process ID Name ParentPID ThreadCount	Event Logs 🔛 MemBrowser 🦹 Bool	kmarks P Search Res	Aults Report	
LiveData Analysis - FiShweta Shama 135.cfs - Constant Constant - Constant	E ListView E Browser Registry Search Hit I I Item(s) selected. Item No : 1 Search Hit ID SI no Process ID Name ParentPID ThreadCount Priority Base	Event Logs 🔛 MemBrowser 🦹 Bool	kmarks 👂 Search Res 2 7 73 5 72 72 14 13	Aults 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).