

# **International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# **TraceQuest: A System Information and Artifact Collection Tool**

Kaushal Kumar Singh 1st.

DY Patil International University, Akurdi, Pune 411044

# ABSTRACT

TraceQuest is a cutting-edge digital forensic tool specifically engineered for live system analysis and incident responses on Windows operating systems. By automating the acquisition of critical system artifacts, TraceQuest enables the rapid assessment of system compromise and user activity. The tool performs an in-depth collection of installed application metadata, including application names, install dates, publisher details, version numbers, and uninstall strings, as well as support and update URLS. It also conducts advanced USB device forensics by leveraging registry analysis to enumerate the connected devices and resolve localised strings for precise device identification. Furthermore, TraceQuest features robust Google Chrome history extraction, ensuring data integrity through temporary database copies to prevent data corruption during live acquisitions. A key feature is the capability to operate in a live forensic environment, thereby minimising the impact on the system while maximising data integrity. TraceQuest provides a user-friendly interface for efficient data retrieval, complemented by comprehensive error handling and detailed logging, making it a valuable asset for digital forensic investigators, incident responders, and system administrators who need to assess and respond to security incidents. The extracted data can be exported to PDF reports, streamlined investigations, and reported workflows.

Keywords: Artifacts, Evidence, Event Logs, Windows Functions, Windows Registry, Forensics.

# 1. INTRODUCTION

Digital forensics is a discipline that is becoming increasingly vital, driven by the continuous rise in the use of digital devices and the resulting surge in cybercrime. The capability to quickly and accurately obtain system data and artifacts is essential for effective incident response, investigation, and threat analysis. Old-fashioned forensic techniques are usually based on the offline examination of disk images, which can take a long time and may be impractical in situations where prompt evaluation of an active system is needed. Live forensics, however, allows investigators to analyse an active system to look for malicious processes, network activity, and the temporary information that could be deleted during a shutdown or imaging procedure.

In this research, I present TraceQuest, a new digital forensic tool that aims to simplify the acquisition of critical system artifacts from live Windows systems. TraceQuest is centred on automating the acquisition of installed application metadata, comprehensive USB device information, and Google Chrome browsing history while ensuring data integrity and reducing the target system's impact.

This utility uses direct registry analysis and temporary database copies to guarantee forensic accuracy and soundness. The gap between extensive forensic analysis and the need for quick incident evaluation gives system administrators and investigators a simple and effective way of comprehending system activity and user behaviour. This article outlines the design, implementation, and functionality of TraceQuest, emphasising its potential to improve live forensic investigations and incident response. This utility uses direct registry analysis and temporary database copies to guarantee forensic accuracy and soundness. The gap between extensive forensic analysis and the need for quick incident evaluation gives system administrators and investigators a simple and effective way of comprehending system activity and user behaviour. This article outlines the design, implementation, and functionality of TraceQuest, emphasising its potential to improve live forensic investigations and incident response activity and user behaviour. This article outlines the design, implementation, and functionality of TraceQuest, emphasising its potential to improve live forensic investigations and incident response processes

\* Kaushl Kumar Singh. Tel.: 7030304288 E-mail address: 20230804030@dypiu.ac.in

## 2. BASICS OF WINDOWS FORENSICS

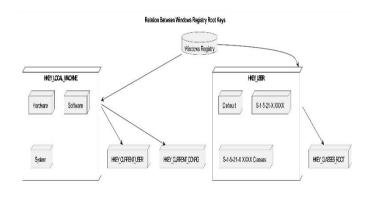
Windows forensic analysis focuses on building in-depth digital forensics knowledge of Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensics capabilities and artifacts is a core component of information security. To recover, analyze and authenticate forensics data on Windows systems, track particular activity on your network and organize findings for use in incident response or internal investigations. Windows is silently recording an unbelievable amount of data about users. It also stores each movement in the system.

### A. Windows Event Logs

Logs are records of events that happen in your computer, either by a person or by running processes. They help you to track what happened and troubleshoot the problems. In any event of Windows investigation, Windows event logs serve as the primary source of evidence as the operating system logs every system activity. Windows event logs can help an investigator draw timeline-based logging information and discover artifacts. An event log contains an abundance of data, which enables for investigation of any abnormal cases or unauthorized access of the system. The investigator can acquire that file in text, and then it will be analyzed using third-party tools like QRadar.

#### B. Windows Registry

For a forensic analyst, the registry is a treasure box of information. It is the database that contains the default settings, user-defined and system-defined settings in a Windows computer. The registry serves as the repository, monitoring, observing and recording the activities performed by the user in the computer. The data is stored in the main folders in a tree-like structure, which is called Hive, and its sub-folders are called Keys and Sub-keys, where each component's configuration is stored and denoted as Values.



# **3. RELATED WORK**

# 2. A. Current tools used to investigate entities, analyze logs and parse registry data

1)Manage Engine Event Log Analyzer, NXLog Agent

#### 2) Windows Live Response

#### B. Limitations of the Current tools used while parsing the registry, investigating entities and analysing logs

- Some tools can only pool standard events like system security applications and setup logs from Windows machines, and don't have the capabilities to pool application and service logs like systems.
- Manage Engine and Event log analysis can collect log-based Windows event channels and can only collect the latest logs generated on the system post-installation.
- 3) Manage Engine, Registry Recon and NXLog Enterprise Edition are paid software for use.

C. The author's initial Windows Forensic tools play a crucial role in collecting and preserving evidence during digital investigations. One notable contribution to this field is the Python-based tool described in the paper, "Forensic Evidence Collection From Windows Host Using Python Based Tool", authored by Mr. Amit Hariyani, Dr. Jaimin Undavia, Dr. Nilay Vaidya and Dr. Atul Patel. This tool introduces an efficient and automated way to collect critical forensic artifacts from Windows systems. While it addresses key challenges in artifact collection, it leaves room for improvement in terms of scope, usability, and modularity.

Feature	Python-Based Tool (Referenced Paper)	TraceQuest
Artifact Coverage	Focused primarily on PowerShell events, Sysmon logs, USB history, and Chrome history.	Expands artifact collection to include network configurations, startup programs, installed applications, and detailed logon sessions.
System Information Collection	Limited system metadata extraction (e.g., OS, date/time).	Comprehensive system-level data, including motherboard, BIOS, CPU, physical memory, and logical disk information.
Network Data Analysis	Not supported.	Includes active network connections, DNS configuration, network adapter details, and routing tables.
Process and Software Insights	Limited.	Provides detailed insights into running processes, task lists, and startup programs.
Interface	Command-line based, requiring higher technical expertise.	User-friendly GUI with categorized buttons and real-time output visualization using Tkinter.
Reporting	Generates text-based outputs.	Automates PDF report generation with customizable examiner details and timestamps.

# 4. PROBLEM SUMMARY

Most of the time, a forensics/incident investigator faces below problems/challenges.

1) The required artifacts are not available on the system

2) If artifacts are available, the investigator doesn't know where to check and how to extract specific artifacts, which can then be investigated in a lab environment

3) Some tools don't have the capabilities to extract specific artifacts, which leads to collecting all the data, which is time-consuming as well as requires more storage for collection and time for investigation

4)Forensics involves gathering data from various sources (system, network, registry, etc.). TraceQuest solves the problem of manually collecting this data by automating the process through WMI queries, registry analysis functions, and file system interactions.

# 5. METHODOLOGY

## 5.1 System Architecture

The tool is implemented in Python, leveraging libraries such as WMI (Windows Management Instrumentation), winreg (Windows Registry API), sqlite3 (SQLite database access), and tkinter (GUI framework). This architecture allows for direct system access while maintaining a low resource footprint on the target system.

The tool's components are organised as follows:

- GUI Interface: Provides user interaction and result display
- Collection Modules: Individual functions for specific artifact collection
- Data Processing: Parsing and formatting collected data
- Reporting: Generating structured reports of findings

#### 5.2 USB Device History Collection

USB device collection methodology extracts information from the Windows registry, specifically targeting the SYSTEM\CurrentControlSet\Enum\USB registry path. This location contains detailed information about USB devices that have been connected to the system, including:

- Device identifiers
- Connection histories
- Hardware details

The collection process accesses the registry using Python's winreg module, traversing the relevant keys to extract device information while handling potential permission issues and access errors.

# 5.3 Web Browser History Collection

For browser history collection, our tool focuses on Google Chrome, one of the most widely used browsers. The collection process involves: 1. Locating the Chrome history database in the user profile

- 2. Creating a temporary copy to avoid database locks
- 3. Querying the SQLite database for URL, title, and timestamp information
- 4. Formatting the results for analysis

The tool handles potential issues such as corrupt databases, access permissions and ensures proper cleanup of temporary files after extraction.

TraceQuest System Information and Art	ifact Collection - O
Physical Memory	
Logical Disk	
Network Info	Chrome Browse History (2025-04-13 17:44:22):
Network Adapter	URL: https://www.amazon.in/gp/css/homepage.html?ref_=nav_youraccount_btn Title: Your Account
Network Adapter Config	Last Visit: 2025-03-27 12:47:55
Active Network Connections	URL: https://www.amazon.in/?&tag=googhydrabk1-21&ref=pd_s1_5szpgfto9i_e&adgrpid=155259813593&hvpone=&hvptwo=&hvadid=674893540034&hvpos=&hvnetw=g&h
Routing Configuration	vrand=72217619358777880838hvqmt=e&hvdev=c&hvdvcmd1=&hvlocint=&hvlocint=%hvlo
DNS Configuration	Last Visit: 2025-03-26 14:05:37
Software & Processes	URL: https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwic5rHoqqeMAxVcpWYCHQNTNdIYABAAGgJzbQ&co=1&gclid=Cj0KCQjwy46_BhDOARIsAIvmcwNBawPEc
Installed Applications	mFBnMDFDTnFCqiUXxWbqJdnNiGr23NISr2LDnuqu0zZeQEaAlvqEALw_wcB&ohost*www.google.com&cid=CAESU-D2qN3eYjbQR13wd-20jytA99DmvHjrxWvhF37tRooybuJnaIOc OA3rLsQm4ArEyeStGU-QYDtciDMcyt0wkJRNGiRirWCpr-unxiHJz20yMH4q&sig=ADO64_2IzIS0jmymu9o_gpiYBAwiYLmvNQ&q&adu/E&ved=2ahUKEwjYlqzoqqMAxUr4zgGHfot
Auto Startup Programs	CZKQQQx8BAgKEAE⋼=7 Title: Online Shopping site in India: Shop Online for Mobiles, Books, Watches, Shoes and More - Amazon.in
Running Processes	Last Visit: 2025-03-26 14:03:52
Task List	URL: https://www.google.com/search?q=MZON&nlz=1C1ONGR_enIN975IN975&oq=MZON&gs_lcrp=EgZjaH3vbWUy8ggAEEUYOdI8CDEzMzFqMGo3qAIAsAIA&sourceid=chrome&id
Task List with Services	"UTF-8 Title: MZON - Google Search
Logon Sessions	Last Visit: 2025-03-26 14:02:31
Artifact Collection	URL: https://web.whatsapp.com/ Title: WhatsApp
USB Device History	Last Visit: 2025-03-26 14:01:55
Chrome Browse History	<pre>URL: https://mail.google.com/mail/u/0/#advanced-search/attach_or_drive=true&amp;query=photo&amp;isrefinement=true?projector=1 Title: mail.google.com</pre>
Extract Event Logs	Last Visit: 2025-03-26 14:01:41
Extract Registry Hives	URL: https://www.instagram.com/pocket_plans/# Title: Pocket plans 🙆 🛸 (@pocket plans) • Instagram photos and videos
Reporting	Last Visit: 2025-03-21 18:43:03
	URL: https://www.instagram.com/pocket plans/reel/DMSg-ATTJ2z/

Fig 5.3.1 Chrome Browser's History

## 5.4 System Information Gathering

Beyond USB and browser artifacts, the tool collects comprehensive system information using WMI queries and command-line utilities:

- Hardware information (motherboard, BIOS, processor)
- Operating system details
- Network configuration
- Running processes and services
- Installed applications
- User account information

System Info	1		
Motherboard	Motherboard Information		
Motherboard			
BIOS		: Base Board : ConfigOptions1, ConfigOptions2, ConfigOptions3, ConfigOptions4, ConfigOptions5, ConfigOptions6, ConfigOpti	
BIUS	Config0ptions Config0ptions8	: Configuptions1, Configuptions2, Configuptions5, Configuptions4, Configuptions5, Configuptions6, Configuption	ons/,
Boot Configuration		: Win32 BaseBoard	
boot conngulation	Description	: Hase Board	
Processor(cpu)	HostingBoard	: True	
(incessor(eps)	HotSwappable	False	
CsProduct	Manufacturer	HP .	
	Name	: Base Board	
Operating System	PoweredOn	: True	
	Product	: 8709	
Date and Time		: False	
	Replaceable	: True	
System User Details		: False	
	SerialNumber	: PKYWP028JFGCEM	
Physical Memory	Status	: OK	
	Tag	: Base Board	
Logical Disk	Version	: 34.37	
Network Info			
Network Adapter			
Network Adapter Config	BIOS Information (2025-0		
Network Adapter Config		: 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43	
Active Network Connections	BIOSCHAPACTERISTICS	: /, 11, 12, 13, 10, 19, 20, 21, 22, 23, 24, 23, 27, 30, 52, 53, 40, 42, 43 : HPQOEM - 2, F.46, INSYDE Corp F46000	
Active Network Connections		: F.46	
Routing Configuration		: en[US]iso8859-1.0	
noting conignition	Description	: F.46	
DNS Configuration	EmbeddedControllerMajor		
	EmbeddedControllerMinor	Version: 37	
Software & Processes	InstallableLanguages	: 5	
	ListOfLanguages	: en US iso8859-1,0, fr FR iso8859-1,0, es ES iso8859-1,0, zh TW unicode,0, zh CN unicode,0	
Installed Applications	Manufacturer	: Insyde	
	Name	: F.46	
Auto Startup Programs	PrimaryBIOS	: True	
	ReleaseDate	: 20240509000000.000000+000	
Running Processes	SerialNumber	: 5CD130CLG9	
	SMBIOSBIOSVersion	: F.46	

# Fig 5.4.1 System Information

# 5.5 Registry and Event Log Export

To facilitate deeper forensic analysis, the tool includes functionality to export Windows registry hives and event logs:

- Registry hives (SYSTEM, SOFTWARE, SAM, SECURITY)
- Windows event logs (System, Application, Security)

These exports are saved with timestamps and proper documentation to maintain the chain of custody.

TraceQuest System Information and Arti	fact Collection —	Ø	×
Physical Memory	[OK] 'OfficeChannel' backed up to: F:/EventLogBackups\OfficeChannel_20250413_174625.evtx [OK] 'OfficeDebugChannel' backed up to: F:/EventLogBackups\OfficeDebugChannel 20250413_174625.evtx		
Logical Disk	[OK] 'OneApp_IGCC' backed up to: F:/EventLogBackups\OneApp_IGCC_20250413_174625.evtx [OK] 'OpenSSH/Admin' backed up to: F:/EventLogBackups\OpenSSH Admin 20250413_174625.evtx		
Network Info	[OK] 'OpenSSH/Debug' backed up to: F:/EventLogBackups\OpenSSH Debug 20250413 174625.evtx [OK] 'OpenSSH/Operational' backed up to: F:/EventLogBackups\OpenSSH Operational 20250413 174625.evtx		
Network Adapter	[OK] 'Physical_Keyboard_Manager_Channel' backed up to: F:/EventLogBackups\Physical_Keyboard_Manager_Channel_20250413_174625.evtx [OK] 'PlayReadyPerformanceChannel' backed up to: F:/EventLogBackups\PlayReadyPerformanceChannel_20250413_174625.evtx		
Network Adapter Config	[OK] 'RTNorkQueueExtended' backed up to: F:/EventLogBackups\RTNorkQueueExtended_20250413_174625.evtx [OK] 'RTNorkQueueTheading' backed up to: F:/EventLogBackups\RTNorkQueueTheading_20250413_174625.evtx		
Active Network Connections	[OK] 'SMSApi' backed up to: F:/EventLogBackups\SMSApi_20250413_174625.evtx [FAIL] Access denied for event log 'Security'. Try running as Administrator.		
Routing Configuration	<pre>[OK] 'Setup' backed up to: F:/EventLogBackups\Setup_20250413_174625.evtx [OK] 'SmbWmiAnalytic' backed up to: F:/EventLogBackups\SmbWmiAnalytic_20250413_174625.evtx</pre>		
DNS Configuration	[OK] 'System' backed up to: F:/EventLogBackups\System_20250413_174625.evtx [OK] 'SystemEventsBroker' backed up to: F:/EventLogBackups\SystemEventsBroker_20250413_174625.evtx		
Software & Processes	[OK] 'TabletPC_InputPanel_channel' backed up to: F:/EventLogBackups\TabletPC_InputPanel_channel_20250413_174625.evtx [OK] 'TabletPC_InputPanel_channel/IHM' backed up to: F:/EventLogBackups\TabletPC_InputPanel_channel_IHM_20250413_174625.evtx		
Installed Applications	<pre>[OK] 'TimeBroker' backed up to: F:/EventLogBackups\TimeBroker_20250413_174625.evtx [OK] 'UIManager_Channel' backed up to: F:/EventLogBackups\UIManager_Channel_20250413_174625.evtx</pre>		
Auto Startup Programs	[OK] 'Uac/Debug' backed up to: F:/EventLogBackups\Uac_Debug_20250413_174625.evtx [OK] 'WINDOWS_KS_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_KS_CHANNEL_20250413_174625.evtx		
Running Processes	[OK] 'WINDOWS_MFH264Enc_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_MFH264Enc_CHANNEL_20250413_174625.evtx [OK] 'WINDOWS_MP4SDECD_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_MP4SDECD_CHANNEL_20250413_174625.evtx		
Task List	[OK] 'WINDOWS_MSMPEG2ADEC_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_MSMPEG2ADEC_CHANNEL_20250413_174625.evtx [OK] 'WINDOWS_MSMPEG2VDEC_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_MSMPEG2VDEC_CHANNEL_20250413_174625.evtx		
Task List with Services	[OK] 'WINDOWS_VCIENC_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_VCIENC_CHANNEL_20250413_174625.evtx [OK] 'WINDOWS_WMPHOTO_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_WMPHOTO_CHANNEL_20250413_174625.evtx		
Logon Sessions	[OK] 'WINDOWS_wmvdecod_CHANNEL' backed up to: F:/EventLogBackups\WINDOWS_wmvdecod_CHANNEL_20250413_174625.evtx [OK] 'WMPSetup' backed up to: F:/EventLogBackups\WMPSetup_20250413_174625.evtx		
Artifact Collection	[OK] 'WMPSyncEngine' backed up to: F:/EventLogBackups\WMPSyncEngine_20250413_174625.evtx [OK] 'Windows Networking Vpn Plugin Platform/Operational' backed up to:		
USB Device History	F:/EventLogBackups\Windows_Networking_Vpn_Plugin_Platform_Operational_20250413_174625.evtx [OK] 'Windows Networking Vpn Plugin Platform/OperationalVerbose' backed up to:		
Chrome Browse History	F:/EventLogBackups\Windows_Networking_Vpn_Plugin_Platform_OperationalVerbose_20250413_174625.evtx [OK] 'Windows PowerShell' backed up to: F:/EventLogBackups\Windows_PowerShell_20250413_174625.evtx		
Extract Event Logs	[OK] 'WordChannel' backed up to: F:/EventLogBackups\WordChannel_20250413_174625.evtx [OK] 'muxencode' backed up to: F:/EventLogBackups\muxencode_20250413_174625.evtx		
Extract Registry Hives	Event Log Backup Summary:		
Reporting	Successfully Backed Up: 1128 Skipped / Not Found: 0		

Fig 5.4.2 Log File Extraction

□ > This PC > KAUSHAL (F:)	> EventLogBackups			Search EventLogBackups	
🛅 🙆 🖻 🕅 🕅 Sort	~ = View ~ ···	•1			🔲 Deta
Name	Date modified	Туре	Size		
AirSpaceChannel_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
AMSI_Debug_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
Analytic_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
Application_20250413_174625	13-04-2025 17:46	Event Log	12,356 KB		
DirectShowFilterGraph_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
DirectShowPluginControl_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
Els_Hyphenation_Analytic_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
EndpointMapper_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
FirstUXPerf-Analytic_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
ForwardedEvents_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
General_Logging_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
HardwareEvents_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
HP_Analytics_20250413_174625	13-04-2025 17:46	Event Log	1,092 KB		
HP_Diagnostics_20250413_174625	13-04-2025 17:46	Event Log	1,092 KB		
IHM_DebugChannel_20250413_174625	13-04-2025 17:46	Event Log	68 KB		
IntelAudioServiceLog 20250413 174625	13-04-2025 17:46	Event Log	68 KB		

Fig 5.4.2 Extracted Log Files

# 6. IMPLEMENTATION

# 6.1 User Interface

The tool employs a two-panel interface:

- Left panel: Categorized buttons for different collection functions
- Right panel: Display area for results and collection status

The interface includes scrollable sections to accommodate various screen sizes and large amounts of collected data. Error handling is integrated to provide feedback on collection status and any issues encountered.

- Jean mino	- System Info			
MetheboardBIOSBIOSCorrigoptionsCorrigoptionsCorrigoptionsCorrigoptionsCorrigoptionsCreation(LassianeProcessor(pu)HotingboardCipronCaperating SystemProcessor(pu)Network InformationSystem User DetailsReplaceableFraceSystem User DetailsReplaceablePhysical MemorySystem User DetailsNetwork Adapter ConfigNetwork Adapter ConfigurationDetailsReplaceableStrial NumberStrial NumberConfigurationDischarterNetwork Adapter ConfigInstalled ApplicationInstalled ApplicationAuto Startup ProgramsReplaceableFinal Adapter StartupStartup ProgramsProductStartup ProgramsPatient Startup ProgramsFinal ReplaceableStartup ProgramsProduct Information (2025-94-13 16:24:29):BioS Information (2025-94-13 16:24:29):BioC Information (2025-94-13 16:24:	- System mo	Motherboard Information	(2025-04-13 16:24:27):	
BIOS       corrigoptions       : Corrigoptions1, Configoptions2, Configoptions3, Configoptions4, Configoptions5, Configoptions7         Boot Configuration       creation(lass)meet       : Win32 BaseBoard         Processor(cpu)       BaseBoard       Description         Active Network Adapter       IP       Base Board         Operating System       PoweredOn       : True         PoweredOn       : True       PoweredOn         PoweredOn       : True         RepuizeBale       : False         RepuizeBale       : False         RepuizeBale       : False         System User Details       : Social Shuber         Version       : Base Board         Version       : Base Board         Version       : Base Board         PoweredOn       : True         RepuizeBale       : False         RepuizeBale       : Social Shuber         BioS Knameter       : Base Board         Version       : Base Board         Po	Motherboard			
Boot Configuration       Configipation 36         Processor(cpu)       Configipation 2         Description 2       Base Board         Operating System       Base Board         Operating System       Processor(cpu)         Date and Time       Base Board         Psychol 2       False         Name       E Base Board         Poperating System       Processor(cpu)         Date and Time       False         Rescription       1         System User Details       Fraise         Physical Memory       1         Logical Disk       Status         Network Adapter       EGS Information (2025-04-13 16:24:29):         Network Adapter       Eios Information (2025-04-13 16:24:29):         Status       10/04-04-04         Disc Information (2025-04-13 16:24:29):         Network Adapter       Eios Information (2025-04-13 16:24:29):         Eios Information (2025-04-13 16:24:29):         Bios Configuration       EinofeedControllerHior/Version: 34         Bios Configuration       EinofeedControllerHior/Version: 34         Bios Configuration       EinofeedControllerHior/Version: 34         BiobedecontrollerHior/Version: 37       EinsteldecontrollerHior/Version: 37         Installed Applications				
Boot ConfigurationCreation ClassifiameHin32 BaseBoardProcesser(cpu)Base BoardTrueAstingBoardTrueOperating SystemPoweredonTrueOperating SystemPoweredonTruePoweredonTruePoweredonTruePoweredonTruePoweredonTruePoweredonEraileResultationEase BoardPoweredonTruePoweredonErailePoweredonEraileResultationEase BoardPoweredonFalseResultationExampleSystem User DetailsEase BoardPhysical MemoryEase BoardStatusE StatusTotalEase BoardWersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardVersionEase BoardBiosCharacteristicsCalicationBiosCharacteristicsCalicationUnstalled ApplicationsEndedecontrollerHonorVersion: 34Auto Statup ProgramsEndedecontrollerHonorVersion: 37Installed ApplicationsEndedecontrollerHonorVersion: 37Installed ApplicationsFriaryBIOSResultFriaryBIOSResultStatusAuto Statup ProgramsErail NubberResult <t< td=""><td>BIOS</td><td></td><td>: ConfigOptions1, ConfigOptions2, ConfigOptions3, ConfigOptions4, ConfigOptions5, ConfigOptions6, ConfigOptio</td><td>ons7,</td></t<>	BIOS		: ConfigOptions1, ConfigOptions2, ConfigOptions3, ConfigOptions4, ConfigOptions5, ConfigOptions6, ConfigOptio	ons7,
Processo(pu)pescription:: Base BoardCoProductHost Suppable: FalseMase:: Base BoardOperating SystemProduct:: 8709Date and Time:: FalseSystem User Details:: FalsePhysical Memory:: FalseLogical Disk:: SastawNetwork Adapter Config:: Base BoardNetwork Adapter Config:: Base BoardNetwork Adapter Config:: SastawNetwork Adapter Config:: FalseSoftware & Processes:: HogOENInstalled Applications:: FalseAuto Statup Programs:: FalseRunning Processes:: FalseRunning Processes:: Softwares EricitiesRunning Processes <td::: ericities<="" softwares="" td="">Running Processes<td::: ericities<="" softwares="" td="">Running Processes<td::: ericities<="" softwares="" td="">Running Processes<td::: ericities<="" softwares="" td="">Running Processes<td:: ericities<="" softwares="" td="">Running</td::></td::></td::></td::></td::></td::></td:::></td:::></td:::></td:::>				
Processor(cpu)HostingBoard: TrueInstingBoard: TrueCcProductHPNamufacturer: HPNamufacturer: HPNamufacturer: HPNamufacturer: HPNamufacturer: HPNamufacturer: HPSystem User Details: FalsePhysical Memory: StatusCommon Status: OKPhysical Memory: StatusNetwork Adapter: BiosCharacteristicsNetwork Adapter Config: HO(255-64-13 16:24:29):Network Adapter Config: HO(255-64-13 16:24:29):Obits Configuration: HO(255-64-13 16:24:29):Distoresion: HO(255-64-13 16:24:29):Distoresion: HO(255-64-13 16:24:29):Installed Applications: HO(255-64-13 16:24:29):Distoresion: HO(255-64-13 16:24:29):Installed Applications: HO(255-64-13 16:24:29):Distoresion: HO(255-64-13 16:24:29):Installed Applications: HO(255-64-13 16:24:29):Distoresion: HO(255-64-13 16:	Boot Configuration			
C2Product       HotSwoppable       : False         Name       Base Board         Operating System       Product       : 8709         Date and Time       Base Board         Product       : 8709         System User Details       False         Physical Memory       : False         Logical Disk       : OK         Network Info       : OK         Network Adapter Config       : Sistem         Network Adapter Config       : Sistem : : Project : Sistem : : : Sistem : : : Sistem : : : Sistem : : : : Sistem : : : : Sistem : : : : : : : : : : : : : : : : : : :	Deservation			
CcProductHamufacturer: HPQuesteding SystemHamufacturer: HPOperating SystemPoweredon: TrueDate and TimeResolution: FalseSystem User Details: FalseSystem User Details: FalsePhysical Memory: Status: OKLogical Disk: Base BoardNetwork Adapter: Base BoardNetwork Adapter Config: Base BoardNetwork Adapter Config: HO(PL)BiosCharacteristics: 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43BiosCharacteristics: enloying in (JSIS859-1, 0)Description: F.46Installed Applications: Enloying in (JSIS859-1, 0, enloying in (JSIS859-1,	Processor(cpu)			
Nameis Base BoardOperating SystemProductis S7.9Date and TimeReplaceableis TrueSystem User DetailsEplaceableis TrueSystem User DetailsSerial Numberis Phylice 20 FGCEHPhysical MemorySerial Numberis Serial NumberLogical DiskVersionis 4.37Network Adapter ConfigElso Information (2025-94-13 16:24:29):Network Adapter ConfigElso Statusis (1, 2, 2, 2, 3, 24, 25, 27, 30, 32, 33, 40, 42, 43)Require Configurationis (1, 2, 2, 2, 3, 24, 25, 27, 30, 32, 33, 40, 42, 43)Require Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 5, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 2, 2, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurationis (1, 2, 2, 2, 24, 25, 27, 30, 32, 33, 40, 42, 43)Configurati	CeBraduct			
Operating SystemPower-edon: TrueDate and TimePower-edon: TrueRemovable: FalseSystem User DetailsEncycle 200Physical MemoryStatus: OKStatus: OKPhysical MemoryTag: Base BoardLogical DiskTrag: Base BoardNetwork AdapterBiostCharacteristics: 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43BiostCharacteristics: enlusion: F46Bouting Configuration: F46: F46DNS Configuration: F46: EnlusionInstalled Applications: IsotCharages <th:: satus<="" th="">Auto Statup Programs: Enlusion: F46Running Processes: SotDistOversion: SotDistCionRunning Processes: SotDistOversion: SotDistCion&lt;</th::>	CSFTODUCT			
Dt and Time       Product       ::::::::::::::::::::::::::::::::::::	Operating System			
Date and Time     Resouble     : False       System User Details     RequiresDaughterBoard     : False       Physical Memory     Status     : OK       Status     : OK       Logical Disk     Tag     : Base Board       Version     : 34.37       Network Adapter     Elios Information (2825-84-13) 16:24:29):       Network Adapter     BiosCharacteristics     : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43       BiosCharacteristics     : 7, 46, 11%SVDE Corp F460000       ONS Configuration     : H00EN     : 7, 46       Distalled Applications     : 7, 46     : 7, 46       Installed Applications     : 7, 46       Auto Statup Programs     : 50138059-1,0     : 50138059-1,0       Running Processes     : 1502     : 746       Running Processes     : 1502     : 746	operating system			
System User Details       Replaceable       : True         Replaceable       : Frue         Physical Memory       : Serial Number         Logical Disk       : Sase Board         Network Info       : Sase Board         Network Adapter       : Social Science Sc	Date and Time			
System User Details     RequiresDaughterBoard     : False       Physical Memory     Status     : DKW0R2376CEH       Logical Dick     Tag     : Sasse Board       Version     : 34.37       Network Adapter     BioSCharacteristics     : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43       Rotuing Configuration     EncodedControllerVision     : F46       DNS Configuration     : EncodedControllerVision     : 746       Installed Applications     : F46       Auto Statup Programs     : F46       Running Processes     : IsoD13000000000000000000000000000000000000	Duce and Time			
Serial Number       : PNYNP0283FGCEN         Logical Disk       : Software Serial Number         Network Info       : Base Board         Network Info       : Software Serial Number         Network Adapter       : Software Serial Number         Network Adapter       : Software Serial Number         Network Connections       : H000EN         Routing Configuration       : H000EN         DNS Configuration       : F.46         Caption <td: 34<="" :="" td="">         Installed Applications       : : : : 10xjde         Manufacturer       : : : : : : : : : : : : : : : : : : :</td:>	System User Details			
Tag       : Base Board         Logical Disk       Version       : 33.37         Network Info		SerialNumber		
Logical Disk       Version       : 34.37         Network Info	Physical Memory	Status	: OK	
Network Info         Network Info         Network Adapter         BiOS Information (2025-06-13 16:24:29):         BiOS Information (2025-06-13 16:24:29):         Active Network Connections         Routing Configuration         DNS Configuration         DNS Configuration         Software & Processes         Installed Applications         Auto Statup Programs         Running Processes         Running Processes         Software B         PrimaryBIOS         Installed Applications         PrimaryBIOS         PrimaryBIOS         Installed Applications         PrimaryBIOS         PrimaryBIOS         Friangle StrialRumber         Softsorter StrialRumber         Stortare StrialRumber         Stortare StrialRumber         Bioschare StrialRumber         Stortare StrialRumber         Stortare StrialRumber         Stortare StrialRumber         Stortare Stortare StriatRumber         Stortare		Tag	: Base Board	
Network Adapter       Network Adapter Config       Active Network Connections       Active Network Connections       Routing Configuration       DNS Configuration       DNS Configuration       DNS Configuration       Software & Processes       Installed Applications       Auto Startup Programs       Running Processes       Running Processes       Software & Programs       Primary BIOS       Final Resolution       Final Resolution       Software & Processes       Installed Applications       Primary BIOS       Final Resolution	Logical Disk	Version	: 34.37	
Network Adapter         Network Adapter Config         Active Network Connections         Active Network Connections         BioSCharacteristics       : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43         BioSCharacteristics       : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43         BioSCharacteristics       : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43         BioSCharacteristics       : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43         BioSCharacteristics       : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43         Disconfiguration       : F, 46         Disconfiguration       : F, 46         Disconfiguration       : InstallableIcanguages         Installed Applications       : Instyle         Auto Statup Programs       : Instyle         Running Processes       : F, 46         PrimaryEDOS       : True         Resconter       : 20240599900000.0000000.0000000.0000000.0000000	Network Info			
Network Adapter Config         Installed Applications           Active Network Connections         Final Book Processes           Routing Configuration         IF.46           DNS Configuration         IF.46           DNS Configuration         IF.46           DNS Configuration         IF.46           Installed Applications         Installed Applications           Auto Starup Programs         instglessore           Running Processes         Instglessore           Running Processes         Instglessore           Running Processes         Isola Starup Programs           PrimaryBIOS         ITrue           ReleaseStare         ISOL Seconder Seco	Network Adapter			
Active Network Connections         BiosCharacteristics         : 7, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 27, 30, 32, 33, 40, 42, 43           BiosCharacteristics         : HPQORM         2, F.46, INSVDE Corp F466000           DNS Configuration         : EnclosedControllerVinorVersion: 34           EbosCharacteristics         : F.46           Installed Applications         : ListOfLanguage           Auto Startup Programs         : FriamyVBIOS           Running Processes         : 2024559000000.000000.000000.000000.000000.00000				
Active Network Connections     BIDSVersion     : HPQCEM - 2, F.46, INSYDE Corp F460000       Routing Configuration     CurrentLanguage     : EnU[S][so8859-1,0       DNS Configuration     EmbeddedControllerHajorVersion: 34       EmbeddedControllerHajorVersion: 37       Installed Applications     : End(S][so8859-1,0, r]FR[iso8859-1,0, es]ES[iso8859-1,0, zh]TN[unicode,0, zh]CN[unicode,0       Auto Startup Programs     : Insyde       Running Processes     : F.46       Running Processes     : SO139CL69       SerialNumber     : SO139CL69       SerialNumber     : SO139CL69       SerialNumber     : SO139CL69	Network Adapter Config			
Routing Configuration     : F_46       DNS Configuration     : F_46       Software & Processes     : Istoffiangeses : 5       Installed Applications     : Istoffiangeses : 5       Auto Startup Programs     : T_46       Running Processes     : SO13902.09       Running Processes     : SO13902.09       Software & Programs     : SO13902.09       Software & Frequest     : SO13902.09       Software & Programs     : SO13902.09       Software & Frequest     : SO13902.09       Software & Programs     : SO13902.09       Software & Frequest     : SO13902.09       Serial Number <td: so13902.09<="" td=""></td:>	Anti-a Maturali Consections	Bioscharacteristics	: /, 11, 12, 15, 16, 19, 20, 21, 22, 23, 24, 25, 2/, 30, 32, 33, 40, 42, 43	
Routing Configuration     : CurrentLanguage : en US 1s08859-1,0       DNS Configuration     : F.46       DNS Configuration     : S       Installed Applications     : S       Auto Startup Programs     : Ensyde       PrimaryBIOS     : True       Running Processes     : SO1390CL69       SoftBarrer     : SO1290CL69       SoftBorrer     : SO1290CL69       Serial Number     : SO1290CL69       SoftBorrer     : SO1290CL69	Active Network Connections			
DNS Configuration         Description         : F.46           EmbeddedControllerHinorVersion:         34           EnbeddedControllerHinorVersion:         34           Installed Applications         ListOfLanguages         :5           Auto Startup Programs         PrimaryBIOS         : Tris           Running Processes         : 50013902.09         :0000000.000000.000000.000000.000000.0000	Pouting Configuration	Current anguage		
DNS Configuration         EmbeddedControllerMsjorversion: 34           EmbeddedControllerMsjorversion: 37         TrastallableLanguages : 5           Installed Applications         Software & Processes           Installed Applications         : enl(U)[is08859-1,0, fr FR is08859-1,0, es ES is08859-1,0, zh TW unicode,0, zh CN unicode,0           Auto Startup Programs         : Fride           Running Processes         : 570139CL69           SerialNumber <td: 570139cl69<="" td="">           SerialNumber         <td: 570139cl69<="" td="">           SerialNumber         <td: 570139cl69<="" td=""></td:></td:></td:>	Routing Configuration	Description		
- Software & Processes Installed Applications Auto Startup Programs PrimaryBIDS : True Running Processes Serial Number : 50139CL69 Serial Number : 50139CL69 S	DNS Configuration			
- Software & Processes InstallableLinguages : 5 ListOfLinguages : 5 ListOfLinguages : 6 ListOfLinguages : 6 ListOfLinguages : 6 ListOfLinguages : 7 ListOfLinguages :	erre comgunation			
ListOfLanguages     : enUtSjiso8859-1,0, fr FR iso8859-1,0, es ES iso8859-1,0, zh TN unicode,0, zh CN unicode,0       Installed Applications     Manufacturer     : Insyde       Auto Startup Programs     Primary8105     : True       ReleaseDate     : 2024950900000,000000+000       SerialNumber     : 5C0130CL09       SerialNumber     : F.46	Software & Processes			
Installed Applications Manufacturer : Insyde Name : F.46 Auto Startup Programs PrimaryBIOS : True ReleaseOate : 20240599000000.000000+000 SreitalNumber : 50130CL09 SreitalNumber : F.46				
Name         :         F.46           Auto Startup Programs         Primary8105         :         True           ReleaseDate <td:2240550900000.000000+000< td="">         :         20240550900000.000000+000           Running Processes         SerialNumber         :         2024050900000.000000+000           Stritt Sold Sold Sold Sold Sold Sold Sold Sold</td:2240550900000.000000+000<>	Installed Applications			
Auto Startup Programs         PrimaryEIOS         : True           ReleaseOate         : 2024056900000.00000+000         : 2024050900000.00000+000           Running Processes         : SroI.30CL09         : 5/0L30CL09           SVBIDGEOSVErsion         : F.4.6         : F.4.6	1.1			
ReleaseDate         : 20240509000000.000000+000           Running Processes         SerialNumber         : SCD130CL09           SWB1050SVersion         : F.46	Auto Startup Programs	PrimaryBIOS		
SMBIOSBIOSVersion : F.46			: 20240509000000.000000+000	
	Running Processes	SerialNumber	: 5CD130CLG9	
			: F.46	

Fig 6.1.1 User Interface

#### **6.2 Key Implementation Features**

The core system handles basic operations and provides foundational services to the specialized modules. Key components include:

import os import winreg import sqlite3 import shutil import tempfile from datetime import datetime import tkinter as tk from tkinter import ttk from tkinter import simpledialog, messagebox, filedialog import wmi import re import subprocess from reportlab.lib.pagesizes import letter from reportlab.pdfgen import canvas from reportlab.platypus import Paragraph, Table, TableStyle from reportlab.lib.styles import getSampleStyleSheet, ParagraphStyle from reportlab.lib.enums import TA\_LEFT, TA\_CENTER from reportlab.lib import colors The implementation leverages several key Python libraries:

winreg **for** Registry access wmi **for** Windows Management Instrumentation queries sqlite3 **for** database interactions subprocess **for** executing system commands Reportlab **for** PDF report generation

The USB device information collection function demonstrates the tool's approach to registry access and error handling. Similar methodologies are applied to other collection functions.

# def gather\_usb\_device\_info(): """ Gathers USB device information from the registry and returns it.""" usb\_info = [] try: registry\_path = r"SYSTEM\CurrentControlSet\Enum\USB" registry = winreg.OpenKey(winreg.HKEY\_LOCAL\_MACHINE, registry\_path) for i in range(winreg.QueryInfoKey(registry)[0]): try: sub\_key\_name = winreg.EnumKey(registry, i) usb\_info.append(f"Device Key Root: {sub\_key\_name}") except OSError: continue # Handle potential permission issues with subkeys winreg.CloseKey(registry) return usb\_info if usb\_info else ["No USB device information found in registry path."] except Exception as e:

return [f"[!] Error gathering USB Device Information: {e}"]

# For Chrome history collection:

def collect\_chrome\_history():
 """Copies Chrome history DB, collects history, and returns it."""
 history\_data = []
 try:

```
home_dir = os.path.expanduser("~")
     db path original = os.path.join(
       home dir,
                        r"AppData\Local\Google\Chrome\User Data\Default\History"
     )
 if not os.path.exists(db path_original):
       return "[!] Chrome history database not found. Is Chrome installed?"
# Create a temporary copy to avoid database lock issues
     temp dir = tempfile.gettempdir()
     temp_db_path = os.path.join(temp_dir, "chrome history temp.db")
     shutil.copy2(db path original, temp db path)
     conn = sqlite3.connect(temp db path)
     cursor = conn.cursor()
     cursor.execute(
       "SELECT url, title, datetime(last visit time/1000000-11644473600, 'unixepoch', 'localtime') as last visit FROM urls ORDER BY last visit time
DESC"
     )
     rows = cursor.fetchall()
     conn.close()
     for row in rows:
       history_data.append({
         "url": row[0],
         "title": row[1] if row[1] else "No Title",
         "last visit": row[2]
       })
     # Clean up temporary file
```

if os.path.exists(temp\_db\_path):

# os.remove(temp\_db\_path)

return history\_data

# except Exception as e:

return f"[!] Error in collecting Chrome History: {e}"

This implementation demonstrates the handling of database connections, SQL queries for artifact extraction, and proper resource cleanup.

# **6.3 Report Generation**

The tool generates structured PDF reports using ReportLab, preserving the formatting and organization of collected data:

- 1. Examiner identification for chain of custody
  - 2. Timestamps for each collection activity
  - 3. Categorized presentation of findings
  - 4. Proper pagination and formatting.

# 7. EVALUATION

#### 7.1 Performance Analysis

The tool was evaluated on multiple Windows systems (Windows 10 and Windows 11) with varying hardware configurations. Key performance metrics included:

- Collection time for each artifact type
- Resource utilization during collection
- Accuracy of collected data compared to manual extraction

Testing revealed efficient performance, with most collection operations completing within seconds to minutes, depending on system size and artifact volume.

#### 7.2 Data Accuracy

Validation testing compared the tool's output with manually extracted artifacts using native Windows tools and commercial forensic solutions. The comparison confirmed the accuracy of:

- USB device identifiers and connection history
- Chrome browsing history entries and timestamps
- System configuration details
- Registry and event log exports

## 7.3 Use Case Scenarios

The tool was applied to several forensic scenarios:

- 1. Data Exfiltration Investigation: Identifying USB devices connected during suspicious periods
- 2. User Activity Analysis: Reconstructing web browsing activity in insider threat cases
- 3. System Compromise Assessment: Gathering system configuration and running processes for malware analysis

In each scenario, the tool successfully collected relevant artifacts for further analysis.

# 8. Limitations and Future Work

While the tool provides valuable forensic capabilities, several limitations exist:

- 1. Limited to locally accessible systems (no remote collection)
- 2. Currently only supports Chrome browser history (not Firefox, Edge, etc.)
- 3. USB device history collection could be expanded to include more detailed connection timestamps

## Future work will address these limitations by:

- 1. Adding support for additional browsers
- 2. Enhancing USB artifact collection with connection timestamps from event logs
- 3. Implementing basic analysis functionality for common investigation types
- 4. Adding support for remote system collection

# 9. CONCLUSION

The enhanced forensic tool presented in this paper provides digital investigators with an effective means of collecting critical artifacts from Windows systems. By focusing on USB device history and web browsing activities while maintaining comprehensive system information collection, the tool addresses common investigative needs.

The open-source nature of the tool allows for customization and validation, important factors in forensic tool acceptance. The structured reporting capabilities ensure proper documentation for evidentiary purposes.

This work contributes to the digital forensics field by demonstrating practical implementations of forensic collection methodologies in a unified, accessible tool that can be deployed in real-world investigations.

# **10. ACKNOWLEDGEMENT**

This Python-based tool is a part of **Forensic Artifacts Collection from Windows Host.** The objective of the consecutive article is to examine Windows file systems, registry, event logs, system monitoring, web browser history, and active network connections for analysis to help the investigator. Windows artifacts are very crucial evidence that is useful for the investigation of USB registries, registry runs, etc. Though this tool is currently built to collect windows registry, event logs, browser history, and network connections but additional capabilities can be added to this by leveraging python modules such as gathering additional details from windows host like recycle bin, running processes, and other event logs; forwarding data to centralized servers and streaming real-time events to SIEM platform. Also collecting data from Linux/Unix and Mac OS-based systems.

# REFERENCES

[1] Hariyani, A., & Undaiva, J. (2022). Forensic Evidence Collection from Windows Host Using Python-Based Tool. In 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA). DOI: 10.1109/ICCCMLA56841.2022.9989295.

- [2] B. Carrier, "File System Forensic Analysis," Addison-Wesley Professional, 2005.
- [3] H. Carvey, "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10," Syngress, 2016.
- [4] E. Casey, "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet," Academic Press, 2011.

[5] OpenText, "EnCase Forensic," [Online]. Available: https://www.opentext.com/products/encase-forensic

[6] AccessData, "Forensic Toolkit (FTK)," [Online]. Available: https://www.exterro.com/forensic-toolkit

[7] N. Agrawal and N. Giramkar, "Forensic Evidence Collection From Windows Host Using Python Based Tool," In 2022 Fourth International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 1208-1213, IEEE, 2022.

[8] J. Collie, "The Windows registry as a forensic resource," Digital Investigation, vol. 10, no. 2, pp. 157-165, 2013.

[9] S. Lim, B. Ahn, and K. Lee, "Windows Registry Analysis for MAC Times," International Conference on Information Security and Assurance, pp. 574-578, 2008.

[10] S. Garfinkel and D. Cox, "Finding and Archiving the Internet Footprint," Digital Lives Research Conference, 2009.