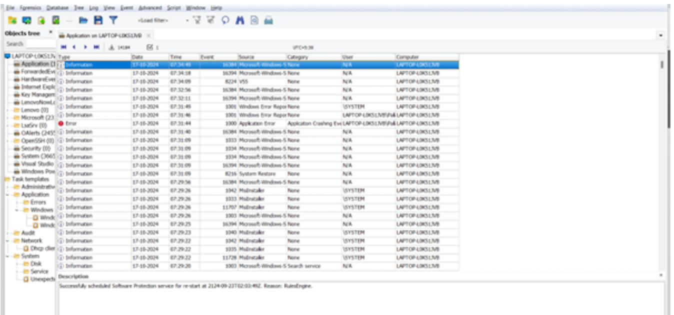
Analysis of various log tools for Digital Forensics

***Abstract*—In the realm of digital forensics and system administration, effective log management and analysis are crucial for maintaining system integrity, diagnosing operational issues, and investigating potential security breaches. Tools such as Event Log Explorer, LogViewPlus, Logwatch, and Gnome Logs offer comprehensive solutions for managing and analyzing logs across different environments and platforms. Event Log Explorer provides robust capabilities for monitoring and filtering Windows event logs, making it a valuable asset for system administrators and forensic experts. LogViewPlus supports a wide range of log formats and offers advanced features for live monitoring and log parsing, enhancing the ability to track application and system behavior. Logwatch, a command-line utility in Kali Linux, generates detailed summaries from system logs, assisting in efficient anomaly detection and investigation. Gnome Logs, also available in Kali Linux, offers a user-friendly graphical interface for quick access and categorization of logs, aiding in troubleshooting and digital forensic analysis. This paper provides a detailed examination of these tools, focusing on their functionalities, features, and applications in the field of digital forensics**

I. windows Tools explanation

II. Event Log Explorer

Event Log Explorer is a comprehensive software solution designed to manage and analyze Windows event logs. It assists system administrators and forensic analysts in monitoring events on both local and remote Windows systems, thus playing a critical role in digital forensics.



Type	Date	Time	Event	Source	Category	User	Computer
Information	17-10-2024	07:34:49	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:34:18	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:34:09	8224	VSS	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:32:56	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:32:11	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:49	1001	Windows Error Repor	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:46	1001	Windows Error Repor	None	LAPTOP-L0KS1JVB\Pal	LAPTOP-L0KS1JVB
Error	17-10-2024	07:31:44	1000	Application Error	Application Crashing Eve	LAPTOP-L0KS1JVB\Pal	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:40	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	1033	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	1034	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	1034	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	8216	System Restore	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:56	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:26	1042	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:26	1033	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:26	11707	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:26	1003	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:25	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:23	1040	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:22	1042	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:22	1035	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:22	11728	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:20	1003	Microsoft-Windows-S	Search service	N/A	LAPTOP-L0KS1JVB

Description

Successfully scheduled Software Protection service for re-start at 2124-09-23T02:03:49Z. Reason: RulesEngine.

Fig. 1. Interface of Event Log Explorer showing event log filtering.

III. Overview of Event Log Explorer

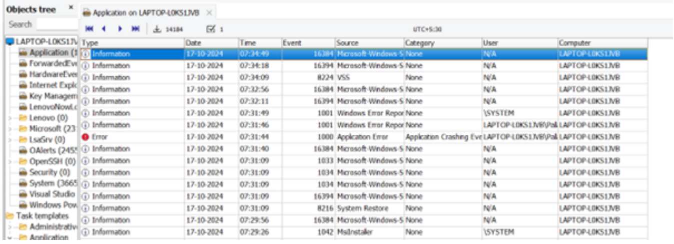
A. Purpose

Event Log Explorer is utilized to monitor, view, and analyze events on Windows systems. It is essential for maintaining system security, diagnosing issues, and conducting digital forensic investigations.

B. Functionality

Event Log Explorer connects to the Windows Event Log Service and retrieves logs from multiple sources, including:

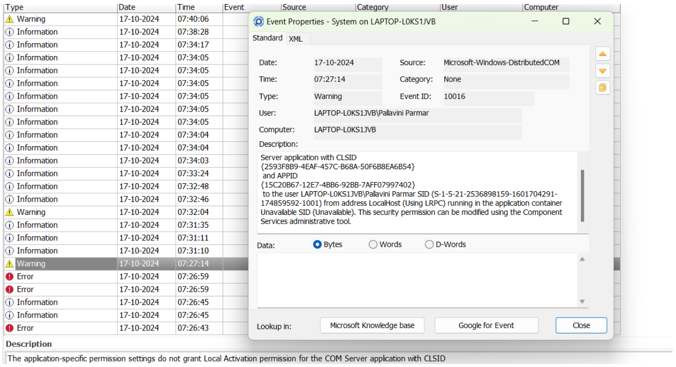
- Application logs



Type	Date	Time	Event	Source	Category	User	Computer
Information	17-10-2024	07:34:49	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:34:18	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:34:09	8224	VSS	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:32:56	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:32:11	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:49	1001	Windows Error Repor	None	\SYSTEM	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:46	1001	Windows Error Repor	None	LAPTOP-L0KS1JVB\Pal	LAPTOP-L0KS1JVB
Error	17-10-2024	07:31:44	1000	Application Error	Application Crashing Eve	LAPTOP-L0KS1JVB\Pal	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:40	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	1033	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	1034	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	1034	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	16394	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:31:09	8216	System Restore	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:56	16384	Microsoft-Windows-S	None	N/A	LAPTOP-L0KS1JVB
Information	17-10-2024	07:29:26	1042	MsiInstaller	None	\SYSTEM	LAPTOP-L0KS1JVB

Fig. 2. Interface of Event Log Explorer showing event log filtering.

- Security logs
- System logs



Type	Date	Time	Event	Source	Category	User	Computer
Warning	17-10-2024	07:40:06					
Information	17-10-2024	07:38:28					
Information	17-10-2024	07:34:17					
Information	17-10-2024	07:34:05					
Information	17-10-2024	07:34:05					
Information	17-10-2024	07:34:05					
Information	17-10-2024	07:34:05					
Information	17-10-2024	07:34:05					
Information	17-10-2024	07:34:05					
Information	17-10-2024	07:34:04					
Information	17-10-2024	07:34:04					
Information	17-10-2024	07:34:03					
Information	17-10-2024	07:33:24					
Information	17-10-2024	07:32:48					
Information	17-10-2024	07:32:46					
Warning	17-10-2024	07:32:04					
Information	17-10-2024	07:31:35					
Information	17-10-2024	07:31:11					
Information	17-10-2024	07:31:10					
Warning	17-10-2024	07:27:14					
Error	17-10-2024	07:26:59					
Error	17-10-2024	07:26:59					
Information	17-10-2024	07:26:45					
Information	17-10-2024	07:26:45					
Error	17-10-2024	07:26:43					

Date: 17-10-2024
Source: Microsoft-Windows-DistributedCOM
Time: 07:27:14
Category: None
Type: Warning
Event ID: 10016
User: LAPTOP-L0KS1JVB\Pallavini Parmar
Computer: LAPTOP-L0KS1JVB
Description:
Server application with CLSID
{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}
and APPID
{15C20B67-12E7-4BB6-92BB-7AFF07997402}
to the user LAPTOP-L0KS1JVB\Pallavini Parmar SID (S-1-5-21-2536898159-1601704291-174859592-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

Data: ● Bytes ○ Words ○ D-Words

Description

The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

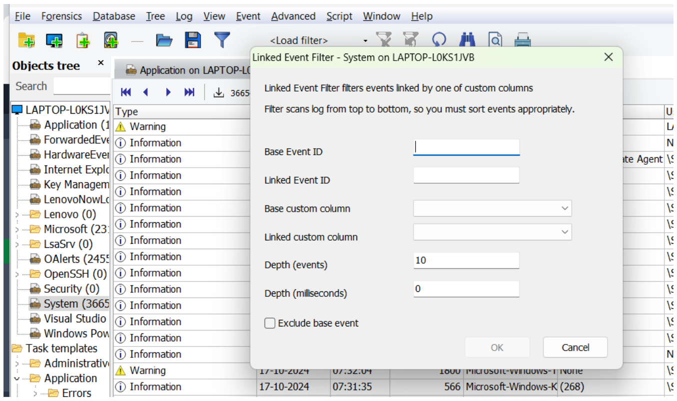
Fig. 3. Interface of Event Log Explorer showing event log filtering.

These logs provide insights into software behavior, security events, and system operations.

IV. Features

Event Log Explorer includes several features to facilitate effective log analysis:

- **Search, Filter, and Group Logs:** Allows for refined searches and filtering to locate specific events.
- **Bookmarking Important Events:** Key events can be bookmarked for quick access.
- **Exporting Logs:** Supports exporting logs to HTML, PDF, and Excel formats for reporting.
- **Multiple Viewing Options:** Includes options for side-by-side comparison of logs for deeper analysis.



Linked Event Filter - System on LAPTOP-L0KS1JVB

Linked Event Filter filters events linked by one of custom columns

Filter scans log from top to bottom, so you must sort events appropriately.

Base Event ID

Linked Event ID

Base custom column

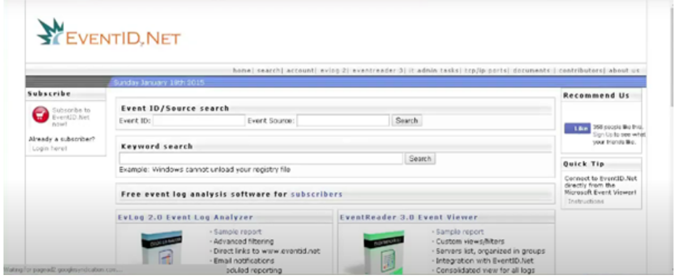
Linked custom column

Depth (events): 10

Depth (milliseconds): 0

☐ Exclude base event

Fig. 4. Interface of Event Log Explorer showing event log filtering.


EVENTID.NET
home | search | account | evlog 2 | eventreader 3 | it admin tasks | tcp/ip ports | documents | contributors | about us
Sunday January 18th 2015
Subscribe
Subscribe to EventID.Net now!
Already a subscriber?
Login here!
Search
Search
Recommend Us
Like
Quick Tip
Instructions

Event ID/Source search

Event ID: Event Source:

Keyword search

Example: Windows cannot unload your registry file

Free event log analysis software for subscribers

EvLog 2.0 Event Log Analyzer

- Sample report
- Advanced filtering
- Direct links to www.eventid.net
- Email notifications
- ...eduled reporting

EventReader 3.0 Event Viewer

- Sample report
- Custom views/filters
- Servers list, organized in groups
- Integration with EventID.Net
- Consolidated view for all logs

Connect to EventID.Net directly from the Microsoft Event Viewer!

Fig. 5. Interface of Event Log Explorer showing event log filtering.

V. Log Exploration and Analysis

A. Log Exploration

Event Log Explorer provides direct access to the Windows Event Log Service, enabling users to pull logs from categories like Security and System logs. Users can explore these logs with detailed information such as event IDs, timestamps, and user actions, aiding in forensic investigations.

B. Log Analysis

The tool supports both real-time and historical log analysis. It allows for tracking and correlating events, identifying trends, and investigating suspicious activities. This capability is crucial for digital forensics as it enables experts to reconstruct timelines and trace actions on compromised systems.

VI. Advantages and Disadvantages

A. Advantages

- **Ease of Use:** The tool is user-friendly, suitable for both non-technical users and advanced system administrators.
- **Efficiency:** Capable of managing and filtering large volumes of logs efficiently.
- **Real-Time and Historical Analysis:** Supports both proactive monitoring and in-depth historical analysis.

B. Disadvantages

- **Limited Advanced Search Capabilities:** Lacks advanced search and correlation features compared to other specialized tools.
- **Platform Limitation:** Supports only Windows platforms, restricting use in mixed operating system environments.

VII. Application in Digital Forensics

Event Log Explorer is highly useful in digital forensics:

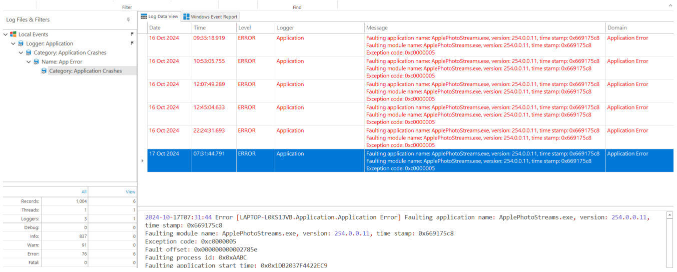
- It enables experts to track unauthorized activities by providing detailed log information.
- It supports exporting logs for evidence preservation and reporting.
- Bookmarking and categorization help in building structured timelines, which are crucial for forensic investigations.

VIII. Conclusion

Event Log Explorer is a valuable tool for both system administration and digital forensics. Despite some limitations, its ease of use and efficiency in handling large log volumes make it an effective solution for Windows event log analysis.

IX. LogViwePlus

LogViewPlus is a versatile software solution developed to manage and analyze log files generated by different systems. It supports various formats, making it suitable for system administrators and forensic analysts to visualize and interpret logs, playing a critical role in digital forensics.



Date	Time	Level	Logger	Message	Domain
16 Oct 2024	09:35:18.919	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	10:53:05.755	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	12:07:49.289	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	12:45:04.633	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
16 Oct 2024	22:24:31.693	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error
17 Oct 2024	07:31:44.791	ERROR	Application	Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8 Exception code: 0xc0000005	Application Error

	All	View
Records:	1,004	6
Threads:	1	1
Loggers:	3	1
Debug:	0	0
Info:	837	0
Warn:	91	0
Error:	76	6
Fatal:	0	0

```
2024-10-17T07:31:44 Error [LAPTOP-L0KS1JVB.Application.Application Error] Faulting application name: ApplePhotoStreams.exe, version: 254.0.0.11,
time stamp: 0x669175c8
Faulting module name: ApplePhotoStreams.exe, version: 254.0.0.11, time stamp: 0x669175c8
Exception code: 0xc0000005
Fault offset: 0x000000000002785e
Faulting process id: 0x0xAABC
Faulting application start time: 0x0x1DB2037F4422EC9
```

Fig. 6. Interface of LogViewPlus showing log filtering.

X. Overview of LogViewPlus

A. Purpose

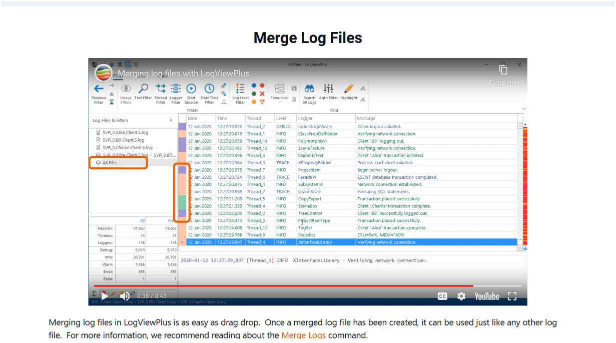
LogViewPlus is utilized for monitoring, viewing, and analyzing logs generated by various applications and systems. It is essential for maintaining system security, diagnosing issues, and conducting digital forensic investigations.

B. Functionality

LogViewPlus supports various log file formats, such as .log, .txt, .csv, and .json. It can also connect to live logs over network protocols like TCP or UDP. This versatility allows users to:

- View application logs
- Analyze system logs
- Monitor live logs in real time

These logs provide insights into software behavior, system events, and application operations.



Merge Log Files

	All	View
Records:	31,663	31,663
Threads:	14	14
Loggers:	116	116
Debug:	9,010	9,010
Info:	20,701	20,701
Warn:	1,456	1,456
Error:	495	495
Fatal:	1	1

Date	Time	Thread	Level	Logger	Message
12 Jan 2020	12:27:19.916	Thread_2	DEBUG	ColorGraphScale	Client logout initiated.
12 Jan 2020	12:27:20.015	Thread_1	INFO	ClassPropDefFolder	Verifying network connection.
12 Jan 2020	12:27:20.058	Thread_14	INFO	PolymorphicVI	Client '.Bill' logging out.
12 Jan 2020	12:27:20.182	Thread_12	INFO	SceneTexture	Verifying network connection.
12 Jan 2020	12:27:20.396	Thread_4	INFO	NumericText	Client '.Alice' transaction initiated.
12 Jan 2020	12:27:20.564	Thread_3	TRACE	XPropertyFolder	Process start client initiated.
2 Jan 2020	12:27:20.575	Thread_7	INFO	ProjectItem	Begin server logout.
2 Jan 2020	12:27:20.734	Thread_6	TRACE	FacadeVI	ESENT database transaction completed.
2 Jan 2020	12:27:20.875	Thread_4	INFO	SubsystemVI	Network connection established.
2 Jan 2020	12:27:20.998	Thread_7	TRACE	GraphScale	Executing SQL statements.
2 Jan 2020	12:27:21.208	Thread_5	INFO	CopyExpert	Transaction placed successfully.
2 Jan 2020	12:27:21.353	Thread_4	INFO	SceneBox	Client '.Charlie' transaction complete.
2 Jan 2020	12:27:22.500	Thread_2	INFO	TreeControl	Client '.Bill' successfully logged out.
2 Jan 2020	12:27:24.414	Thread_5	INFO	ProjectItemType	Transaction placed successfully.
12 Jan 2020	12:27:24.608	Thread_12	INFO	TagSet	Client '.Alice' transaction complete.
12 Jan 2020	12:27:29.766	Thread_8	INFO	Statistics	CPU=54%, MEM=100%
12 Jan 2020	12:27:29.897	Thread_4	INFO	XInterfaceLibrary	Verifying network connection.

```
2020-01-12 12:27:29,897 [Thread_4] INFO  XInterfaceLibrary - Verifying network connection.
```

Merging log files in LogViewPlus is as easy as drag drop. Once a merged log file has been created, it can be used just like any other log file. For more information, we recommend reading about the Merge Logs command.

Fig. 7. LogViewPlus functionality for live log monitoring.

XI. Features of LogViewPlus

LogViewPlus includes several features to facilitate effective log analysis:

- **Log Parsing and Filtering:** Automatically parses logs and allows users to filter based on criteria like keywords or log levels (e.g., ERROR, WARNING, INFO).
- **Log Merging:** Supports merging multiple log files for cross-referencing and deeper analysis.
- **Real-time Monitoring:** Users can monitor logs in real time and receive alerts when specific events occur.
- **Search and Bookmarking:** Advanced search functionality with bookmarking of important log entries for easy access.
- **Exporting Logs:** Allows exporting logs to formats such as HTML, PDF, and CSV for reporting and evidence preservation.

XII. Log Exploration and Analysis

A. Log Exploration

LogViewPlus provides tools for accessing, filtering, and parsing logs from various sources. Users can navigate through logs with details such as timestamps, log levels, and message content, allowing for detailed forensic analysis.

B. Log Analysis

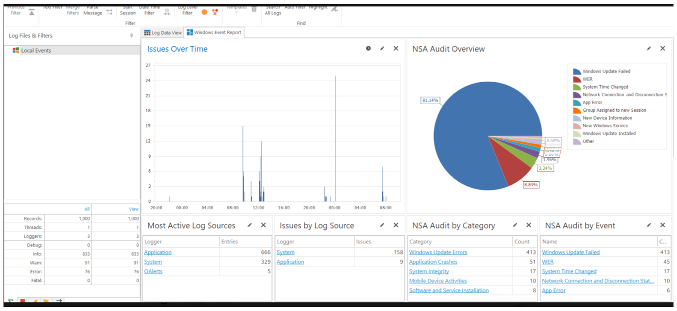
LogViewPlus supports both real-time and historical log analysis. It enables users to track and correlate events across multiple logs, identify patterns, and investigate suspicious behavior. These capabilities are essential for digital forensics, as they help experts reconstruct system activity and user actions.

XIII. Analysis of Log Management Interface

The image presents an interface of a log management and analysis tool, showcasing various log sources, categories, and visualizations for in-depth analysis.

A. Log Files & Filters Pane

The left panel lists the available log files and filters applied during the session. The currently selected log source is **Local Events**, indicating analysis of logs from the local system.



	All	View
Records:	1,000	1,000
Threads:	1	1
Loggers:	3	3
Debug:	0	0
Info:	833	833
Warn:	91	91
Error:	76	76
Fatal:	0	0

Most Active Log Sources

Logger	Entries
Application	666
System	329
OAlerts	5

Issues by Log Source

Logger	Issues
System	158
Application	9

NSA Audit by Category

Category	Count
Windows Update Errors	413
Application Crashes	51
System Integrity	17
Mobile Device Activities	10
Software and Service Installation	8

NSA Audit by Event

Name	C...
Windows Update Failed	413
WER	45
System Time Changed	17
Network Connection and Disconnection Stat...	10
App Error	6

Fig. 8. LogViewPlus features for log analysis and filtering.

B. Main Dashboard

The main dashboard consists of several graphical representations and tables providing an overview of log data:

- **Issues Over Time Chart:** This line graph displays the frequency of issues recorded over time, helping identify patterns and periods of high activity or anomalies.
- **NSA Audit Overview:** The pie chart shows the distribution of events as categorized by an NSA audit. The largest portion is attributed to *Windows Update Failed* (81.14%), suggesting a prevalent issue with updates. Other categories like *System Time Changed* and *App Error* are shown as smaller segments.

C. Most Active Log Sources

The table labeled **Most Active Log Sources** lists the log sources with the highest number of entries:

- **Application**: 666 entries
- **System**: 329 entries
- **OAlerts**: 5 entries

This information assists in determining which sources generate the most logs for further analysis.

D. Issues by Log Source

Another table displays the number of issues recorded per log source:

- **System**: 158 issues
- **Application**: 9 issues

This helps prioritize investigation efforts based on the frequency of issues.

E. NSA Audit by Category

The **NSA Audit by Category** table categorizes events into headings such as *Windows Update Errors* and *Application Crashes*, with counts provided for each. The highest number of events is found under *Windows Update Errors* (413), indicating frequent update-related problems.

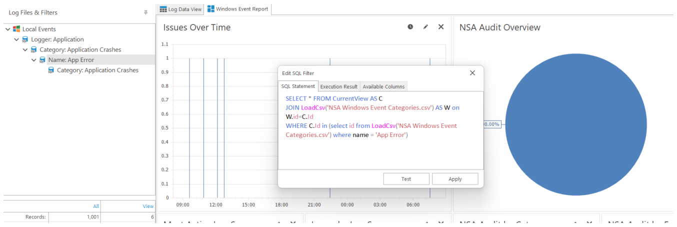
F. NSA Audit by Event

The **NSA Audit by Event** table provides a detailed breakdown of specific events, such as:

- **Windows Update Failed**: 413 occurrences
- **WER (Windows Error Reporting)**: 45 occurrences

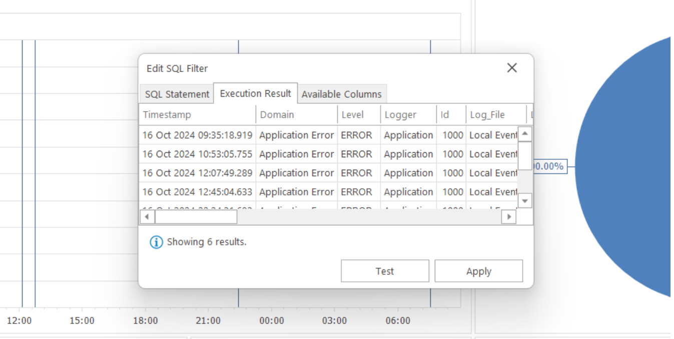
- **System Time Changed**: 17 occurrences

This section allows forensic analysts to focus on specific incidents affecting the system.



```
SELECT * FROM CurrentView AS C
JOIN LoadCsv('NSA Windows Event Categories.csv') AS W on
W.id=C.Id
WHERE C.Id in (select id from LoadCsv('NSA Windows Event
Categories.csv') where name = 'App Error')
```

Fig. 9. Log management interface showing log filtering, visualization, and categorization.



Timestamp	Domain	Level	Logger	Id	Log_File
16 Oct 2024 09:35:18.919	Application Error	ERROR	Application	1000	Local Event
16 Oct 2024 10:53:05.755	Application Error	ERROR	Application	1000	Local Event
16 Oct 2024 12:07:49.289	Application Error	ERROR	Application	1000	Local Event
16 Oct 2024 12:45:04.633	Application Error	ERROR	Application	1000	Local Event

Showing 6 results.

Fig. 10. LogViewPlus interface showing detailed log analysis.

XIV. Advantages and Disadvantages of LogViewPlus

A. Advantages

- **Ease of Use:** LogViewPlus has an intuitive interface, suitable for both technical and non-technical users.
- **Versatility:** Capable of managing various log formats, including text files, CSV, and JSON logs.
- **Real-Time Monitoring:** Supports live log monitoring, making it suitable for proactive monitoring and real-time response.
- **Customizable Filters:** Users can create custom filters and rules for specific log patterns, enhancing log analysis capabilities.

B. Disadvantages

- **Platform Limitation:** LogViewPlus is designed primarily for Windows systems, limiting its use in multi-platform environments.
- **Complex Configuration for Advanced Use:** Setting up advanced features like network log monitoring may require additional configuration steps.

XV. Application in Digital Forensics

LogViewPlus is highly useful in digital forensics:

- It enables forensic experts to monitor and analyze log files efficiently, providing detailed insights into application behavior and system events.
- The tool supports exporting logs in various formats for evidence preservation and further analysis.
- Bookmarking and categorization capabilities allow forensic analysts to build structured timelines, essential for reconstructing incidents.

XVI. kali Tools

A. *Gnome Logs*

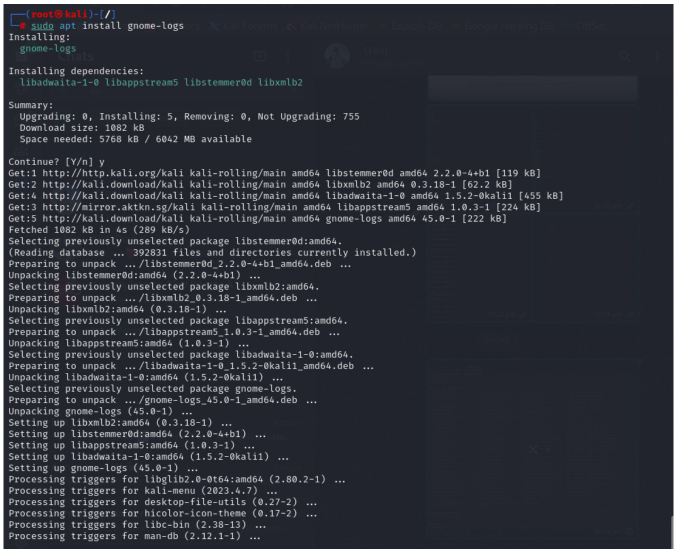
Gnome Logs is a lightweight and intuitive log viewer designed for the GNOME desktop environment. It provides users with an accessible way to manage and view system logs, offering a straightforward approach for troubleshooting and digital forensic analysis, particularly useful in Kali Linux.

B. Installation

To install Gnome Logs on Kali Linux, use the following command:

```
sudo apt install gnome-logs
```

This command installs Gnome Logs and integrates it into the GNOME desktop environment.



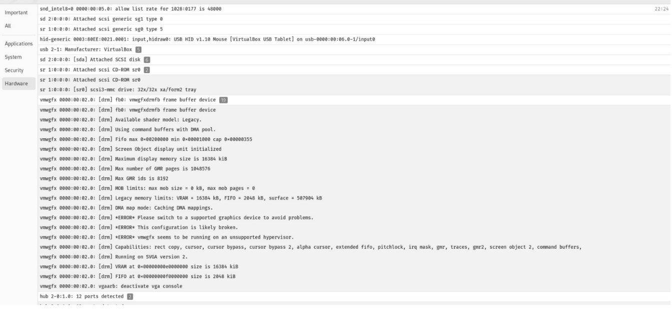
```
┌──(root㉿kali)-[/]
└─# sudo apt install gnome-logs
Installing:
  gnome-logs

Installing dependencies:
  libadwaita-1-0 libappstream5 libstemmer0d libxmlb2

Summary:
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 755
  Download size: 1082 kB
  Space needed: 5768 kB / 6042 MB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libstemmer0d amd64 2.2.0-4+b1 [119 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libxmlb2 amd64 0.3.18-1 [62.2 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libadwaita-1-0 amd64 1.5.2-0kali1 [455 kB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libappstream5 amd64 1.0.3-1 [224 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 gnome-logs amd64 45.0-1 [222 kB]
Fetched 1082 kB in 4s (289 kB/s)
Selecting previously unselected package libstemmer0d:amd64.
(Reading database ... 392831 files and directories currently installed.)
Preparing to unpack .../libstemmer0d_2.2.0-4+b1_amd64.deb ...
Unpacking libstemmer0d:amd64 (2.2.0-4+b1) ...
Selecting previously unselected package libxmlb2:amd64.
Preparing to unpack .../libxmlb2_0.3.18-1_amd64.deb ...
Unpacking libxmlb2:amd64 (0.3.18-1) ...
Selecting previously unselected package libappstream5:amd64.
Preparing to unpack .../libappstream5_1.0.3-1_amd64.deb ...
Unpacking libappstream5:amd64 (1.0.3-1) ...
Selecting previously unselected package libadwaita-1-0:amd64.
Preparing to unpack .../libadwaita-1-0_1.5.2-0kali1_amd64.deb ...
Unpacking libadwaita-1-0:amd64 (1.5.2-0kali1) ...
Selecting previously unselected package gnome-logs.
Preparing to unpack .../gnome-logs_45.0-1_amd64.deb ...
Unpacking gnome-logs (45.0-1) ...
Setting up libxmlb2:amd64 (0.3.18-1) ...
Setting up libstemmer0d:amd64 (2.2.0-4+b1) ...
Setting up libappstream5:amd64 (1.0.3-1) ...
Setting up libadwaita-1-0:amd64 (1.5.2-0kali1) ...
Setting up gnome-logs (45.0-1) ...
Processing triggers for libglib2.0-0t64:amd64 (2.80.2-1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.38-13) ...
Processing triggers for man-db (2.12.1-1) ...
```

Fig. 11. installation

C. Usage

Gnome Logs categorizes logs for easier navigation and analysis. The categorized view includes:

- **System Logs:** Provides insights into the overall system performance, status, and activity.
- **User Logs:** Displays activities and events specific to user actions, helping trace user behavior.
- **Kernel Logs:** Shows kernel-level messages and events, useful for diagnosing system-level issues.



```
snd_intel8x0 0000:00:05.0: allow list rate for 1028:0177 is 48000        22:24
sd 2:0:0:0: Attached scsi generic sg1 type 0
sr 1:0:0:0: Attached scsi generic sg0 type 5
hid-generic 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
usb 2-1: Manufacturer: VirtualBox 5
sd 2:0:0:0: [sda] Attached SCSI disk 6
sr 1:0:0:0: Attached scsi CD-ROM sr0 2
sr 1:0:0:0: Attached scsi CD-ROM sr0
sr 1:0:0:0: [sr0] scsi3-mmc drive: 32x/32x xa/form2 tray
vmwgfx 0000:00:02.0: [drm] fb0: vmwgfxdrmfb frame buffer device 19
vmwgfx 0000:00:02.0: [drm] fb0: vmwgfxdrmfb frame buffer device
vmwgfx 0000:00:02.0: [drm] Available shader model: Legacy.
vmwgfx 0000:00:02.0: [drm] Using command buffers with DMA pool.
vmwgfx 0000:00:02.0: [drm] Fifo max 0x00200000 min 0x00001000 cap 0x00000355
vmwgfx 0000:00:02.0: [drm] Screen Object display unit initialized
vmwgfx 0000:00:02.0: [drm] Maximum display memory size is 16384 kiB
vmwgfx 0000:00:02.0: [drm] Max number of GMR pages is 1048576
vmwgfx 0000:00:02.0: [drm] Max GMR ids is 8192
vmwgfx 0000:00:02.0: [drm] MOB limits: max mob size = 0 kB, max mob pages = 0
vmwgfx 0000:00:02.0: [drm] Legacy memory limits: VRAM = 16384 kB, FIFO = 2048 kB, surface = 507904 kB
vmwgfx 0000:00:02.0: [drm] DMA map mode: Caching DMA mappings.
vmwgfx 0000:00:02.0: [drm] *ERROR* Please switch to a supported graphics device to avoid problems.
vmwgfx 0000:00:02.0: [drm] *ERROR* This configuration is likely broken.
vmwgfx 0000:00:02.0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hypervisor.
vmwgfx 0000:00:02.0: [drm] Capabilities: rect copy, cursor, cursor bypass, cursor bypass 2, alpha cursor, extended fifo, pitchlock, irq mask, gmr, traces, gmr2, screen object 2, command buffers,
vmwgfx 0000:00:02.0: [drm] Running on SVGA version 2.
vmwgfx 0000:00:02.0: [drm] VRAM at 0x00000000e0000000 size is 16384 kiB
vmwgfx 0000:00:02.0: [drm] FIFO at 0x00000000f0000000 size is 2048 kiB
vmwgfx 0000:00:02.0: vgaarb: deactivate vga console
hub 2-0:1.0: 12 ports detected 2
```

Fig. 12. Gnome Logs Interface displaying categorized logs.

D. Features

Gnome Logs offers several features designed for efficient log management:

- **User-friendly Interface:** The clean and intuitive interface enables easy navigation through logs.
- **Categorized Log View:** Logs are organized into categories such as system, user, and kernel logs for quick access.
- **Filtering and Searching:** Users can filter and search specific log entries, making troubleshooting faster.
- **Integration with GNOME:** Gnome Logs seamlessly integrates with the GNOME desktop environment, ensuring a consistent user experience.

E. Advantages

- **Lightweight:** Gnome Logs is lightweight, ensuring minimal system resource usage.
- **Easy Installation:** Simple installation and setup process via the GNOME package manager.
- **Well-integrated with GNOME:** Best suited for users using GNOME-based environments like Kali Linux.

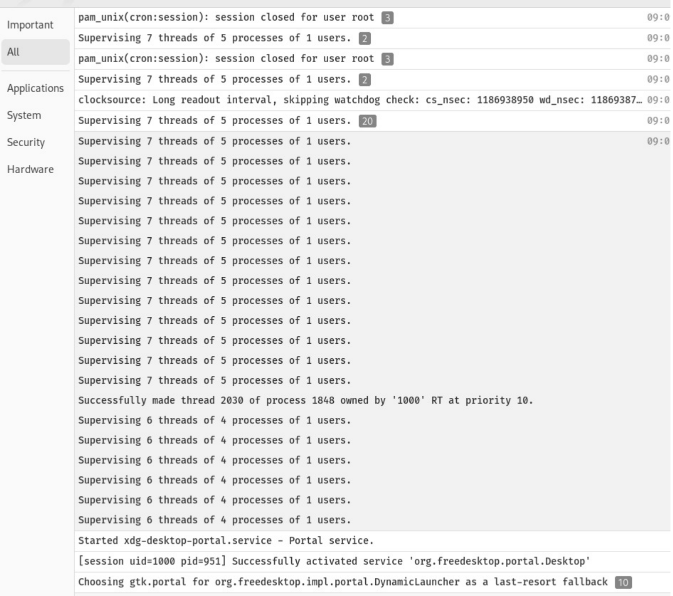
F. Disadvantages

- **Limited Functionality:** Gnome Logs lacks advanced log management capabilities available in other tools.
- **Platform Dependency:** Primarily designed for GNOME, it may not be as effective outside of GNOME-based environments.

G. Application in Digital Forensics

Gnome Logs is particularly useful in digital forensics, especially when working with GNOME-based systems like Kali Linux:

- It allows forensic experts to monitor system, user, and kernel logs, providing insights into system performance and user activities.
- The filtering and search capabilities help in locating suspicious activities and reconstructing events for forensic analysis.
- By categorizing logs, Gnome Logs helps create structured timelines, essential for tracing unauthorized access or abnormal behavior.



```
pam_unix(cron:session): session closed for user root 3                    09:0
Supervising 7 threads of 5 processes of 1 users. 2                        09:0
pam_unix(cron:session): session closed for user root 3                    09:0
Supervising 7 threads of 5 processes of 1 users. 2                        09:0
clocksource: Long readout interval, skipping watchdog check: cs_nsec: 1186938950 wd_nsec: 11869387… 09:0
Supervising 7 threads of 5 processes of 1 users. 20                       09:0
Supervising 7 threads of 5 processes of 1 users.                          09:0
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Supervising 7 threads of 5 processes of 1 users.
Successfully made thread 2030 of process 1848 owned by '1000' RT at priority 10.
Supervising 6 threads of 4 processes of 1 users.
Supervising 6 threads of 4 processes of 1 users.
Supervising 6 threads of 4 processes of 1 users.
Supervising 6 threads of 4 processes of 1 users.
Supervising 6 threads of 4 processes of 1 users.
Supervising 6 threads of 4 processes of 1 users.
Started xdg-desktop-portal.service - Portal service.
[session uid=1000 pid=951] Successfully activated service 'org.freedesktop.portal.Desktop'
Choosing gtk.portal for org.freedesktop.impl.portal.DynamicLauncher as a last-resort fallback 10
```

Fig. 13. Gnome Logs Interface displaying categorized logs.

XVII. Conclusion

Gnome Logs is a practical and accessible tool for log analysis in GNOME environments, such as Kali Linux. While it may not offer the advanced features of specialized log management tools, its lightweight nature, simplicity, and integration with GNOME make it a suitable option for quick troubleshooting and basic digital forensic investigations.

XVIII. kali Tools explanation

A. ***Logwatch***

B. ***Overview***

Logwatch is a powerful log analysis tool that summarizes and reports on various system logs. It processes log files from different sources, providing a comprehensive overview of system activities and security events. This tool is particularly useful for system administrators and forensic analysts who need to monitor system performance and security.

C. ***Installation***

To install Logwatch, run the following command in your terminal:

```
sudo apt install logwatch
```

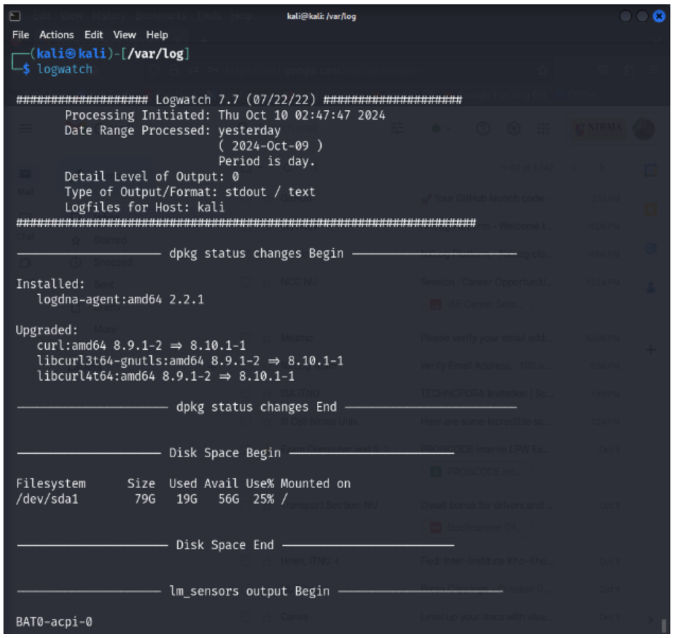
D. ***Usage***

Logwatch can be executed by running:

```
sudo logwatch
```

This command generates a summary of the logs, which can be displayed in the terminal or sent via email, depending on the configuration. Logwatch analyzes various log files, including those from the following sources:

- System logs (e.g., `/var/log/syslog`)



```
┌──(kali㉿kali)-[/var/log]
└─$ logwatch

################### Logwatch 7.7 (07/22/22) ####################
        Processing Initiated: Thu Oct 10 02:47:47 2024
        Date Range Processed: yesterday
                              ( 2024-Oct-09 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: kali
##################################################################

 --------------------- dpkg status changes Begin ------------------------

 Installed:
    logdna-agent:amd64 2.2.1

 Upgraded:
    curl:amd64 8.9.1-2 ⇒ 8.10.1-1
    libcurl3t64-gnutls:amd64 8.9.1-2 ⇒ 8.10.1-1
    libcurl4t64:amd64 8.9.1-2 ⇒ 8.10.1-1

 ---------------------- dpkg status changes End -------------------------


 --------------------- Disk Space Begin ------------------------

 Filesystem      Size  Used Avail Use% Mounted on
 /dev/sda1        79G   19G   56G  25% /


 ---------------------- Disk Space End -------------------------


 --------------------- lm_sensors output Begin ------------------------

 BAT0-acpi-0
```

Fig. 14. logwatch logs.

- Authentication logs (e.g., `/var/log/auth.log`)
- Application-specific logs

E. How It Works

Logwatch works by scanning predefined log files and extracting relevant information. It categorizes the logs into sections, allowing users to quickly identify issues or events of interest. The tool can be customized to include or exclude specific logs, and it formats the output for easy readability.

F. Advantages

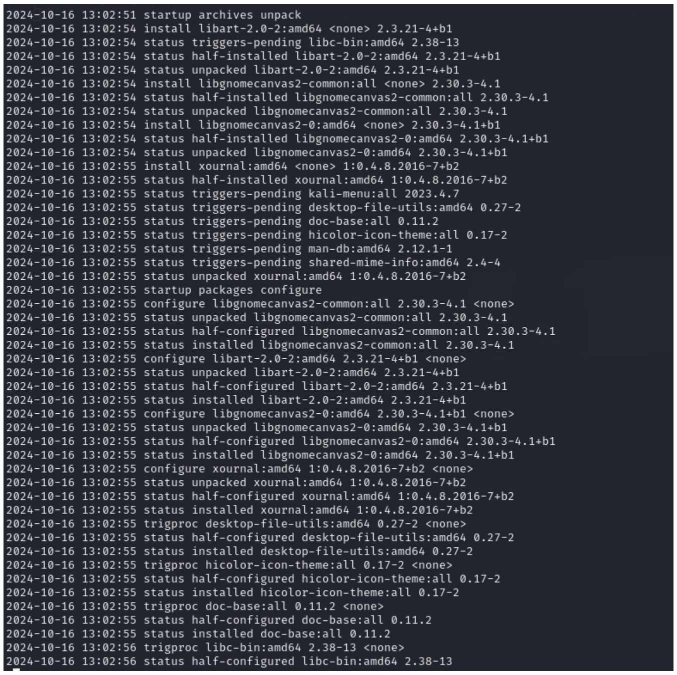
- **Ease of Use:** Logwatch is simple to install and configure, making it accessible for both technical and non-technical users.
- **Automated Reporting:** It can be scheduled to run at regular intervals, providing automated log summaries via email.
- **Comprehensive Analysis:** Logwatch consolidates logs from various sources, offering a holistic view of system activity.

G. Disadvantages

- **Limited Real-Time Monitoring:** Logwatch generates summaries after logs are created, so it may not be suitable for real-time monitoring.
- **Basic Functionality:** Compared to advanced log management tools, Logwatch may lack some features such as in-depth log searching and filtering.

H. Application in Digital Forensics

Logwatch is beneficial in digital forensics due to the following reasons:



```
2024-10-16 13:02:51 startup archives unpack
2024-10-16 13:02:54 install libart-2.0-2:amd64 <none> 2.3.21-4+b1
2024-10-16 13:02:54 status triggers-pending libc-bin:amd64 2.38-13
2024-10-16 13:02:54 status half-installed libart-2.0-2:amd64 2.3.21-4+b1
2024-10-16 13:02:54 status unpacked libart-2.0-2:amd64 2.3.21-4+b1
2024-10-16 13:02:54 install libgnomecanvas2-common:all <none> 2.30.3-4.1
2024-10-16 13:02:54 status half-installed libgnomecanvas2-common:all 2.30.3-4.1
2024-10-16 13:02:54 status unpacked libgnomecanvas2-common:all 2.30.3-4.1
2024-10-16 13:02:54 install libgnomecanvas2-0:amd64 <none> 2.30.3-4.1+b1
2024-10-16 13:02:54 status half-installed libgnomecanvas2-0:amd64 2.30.3-4.1+b1
2024-10-16 13:02:54 status unpacked libgnomecanvas2-0:amd64 2.30.3-4.1+b1
2024-10-16 13:02:55 install xournal:amd64 <none> 1:0.4.8.2016-7+b2
2024-10-16 13:02:55 status half-installed xournal:amd64 1:0.4.8.2016-7+b2
2024-10-16 13:02:55 status triggers-pending kali-menu:all 2023.4.7
2024-10-16 13:02:55 status triggers-pending desktop-file-utils:amd64 0.27-2
2024-10-16 13:02:55 status triggers-pending doc-base:all 0.11.2
2024-10-16 13:02:55 status triggers-pending hicolor-icon-theme:all 0.17-2
2024-10-16 13:02:55 status triggers-pending man-db:amd64 2.12.1-1
2024-10-16 13:02:55 status triggers-pending shared-mime-info:amd64 2.4-4
2024-10-16 13:02:55 status unpacked xournal:amd64 1:0.4.8.2016-7+b2
2024-10-16 13:02:55 startup packages configure
2024-10-16 13:02:55 configure libgnomecanvas2-common:all 2.30.3-4.1 <none>
2024-10-16 13:02:55 status unpacked libgnomecanvas2-common:all 2.30.3-4.1
2024-10-16 13:02:55 status half-configured libgnomecanvas2-common:all 2.30.3-4.1
2024-10-16 13:02:55 status installed libgnomecanvas2-common:all 2.30.3-4.1
2024-10-16 13:02:55 configure libart-2.0-2:amd64 2.3.21-4+b1 <none>
2024-10-16 13:02:55 status unpacked libart-2.0-2:amd64 2.3.21-4+b1
2024-10-16 13:02:55 status half-configured libart-2.0-2:amd64 2.3.21-4+b1
2024-10-16 13:02:55 status installed libart-2.0-2:amd64 2.3.21-4+b1
2024-10-16 13:02:55 configure libgnomecanvas2-0:amd64 2.30.3-4.1+b1 <none>
2024-10-16 13:02:55 status unpacked libgnomecanvas2-0:amd64 2.30.3-4.1+b1
2024-10-16 13:02:55 status half-configured libgnomecanvas2-0:amd64 2.30.3-4.1+b1
2024-10-16 13:02:55 status installed libgnomecanvas2-0:amd64 2.30.3-4.1+b1
2024-10-16 13:02:55 configure xournal:amd64 1:0.4.8.2016-7+b2 <none>
2024-10-16 13:02:55 status unpacked xournal:amd64 1:0.4.8.2016-7+b2
2024-10-16 13:02:55 status half-configured xournal:amd64 1:0.4.8.2016-7+b2
2024-10-16 13:02:55 status installed xournal:amd64 1:0.4.8.2016-7+b2
2024-10-16 13:02:55 trigproc desktop-file-utils:amd64 0.27-2 <none>
2024-10-16 13:02:55 status half-configured desktop-file-utils:amd64 0.27-2
2024-10-16 13:02:55 status installed desktop-file-utils:amd64 0.27-2
2024-10-16 13:02:55 trigproc hicolor-icon-theme:all 0.17-2 <none>
2024-10-16 13:02:55 status half-configured hicolor-icon-theme:all 0.17-2
2024-10-16 13:02:55 status installed hicolor-icon-theme:all 0.17-2
2024-10-16 13:02:55 trigproc doc-base:all 0.11.2 <none>
2024-10-16 13:02:55 status half-configured doc-base:all 0.11.2
2024-10-16 13:02:55 status installed doc-base:all 0.11.2
2024-10-16 13:02:56 trigproc libc-bin:amd64 2.38-13 <none>
2024-10-16 13:02:56 status half-configured libc-bin:amd64 2.38-13
```

Fig. 15. Logwatch Logs Interface displaying categorized logs.

- **Incident Investigation:** It helps forensic analysts identify unusual activities by providing summaries of security events and authentication attempts.
- **Audit Trails:** The summaries generated by Logwatch can serve as a part of the audit trail, assisting in post-incident analysis.
- **Ease of Reporting:** The formatted reports generated by Logwatch can be used as evidence in legal proceedings or security audits.

I. Conclusion

Logwatch is a valuable tool for monitoring and analyzing logs efficiently. While it may have limitations in real-time monitoring and advanced features, its ease of use and automated reporting capabilities make it an effective solution for both system administration and digital forensics.