Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Utilizing Event Logs of Windows Operating System in Digital Crime Investigations

Nagendar Rao Koppolu
Inspector of Police (In-charge State Cyber Vertical),
Telangana Police Department,
Hyderabad, Telangana, India

Abstract **- Microsoft Windows uses Windows Event Logs extensively to store detailed logs of events generated by the operating system, services, and core Windows applications. Many third-party applications also use Windows Event Logs to store details of their internal events. Based on the logged events, certain user actions may also be identified. Hence, analysis of Windows Event Logs is a critical skill required by a digital forensics investigator. While digital forensics products do provide a range of features to examine Windows Event Log entries, an investigator must understand the nature of these entries and the underlying mechanisms. This paper explores these aspects in detail and presents several important Windows Logs areas that are relevant for a digital forensics investigator**

Keywords - Windows Event Log, digital forensics, cybercrime investigation, Microsoft Windows Introduction

I. INTRODUCTION

A. Windows Architecture:

Within Windows operating system, kernel and user mode applications reside. User-mode applications are accessed using Windows Shell components. Windows kernel is a low-level program that interacts with hardware drivers and creates application processes that use hardware resources. It includes accessing applications and their data (primarily files and folders).

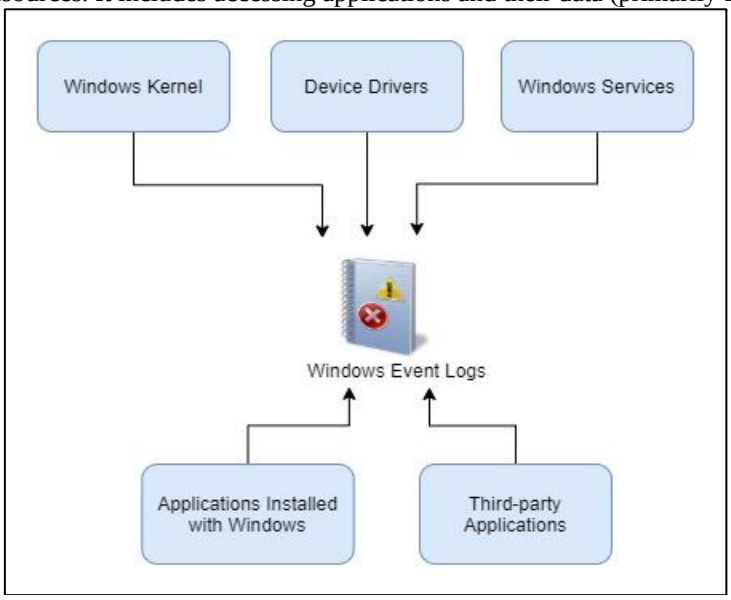

Fig. 1: Windows Event Log and its interactions with Windows components and applications

All the critical components of Windows and its core applications use the Windows Event Log mechanism to store details of their events. Windows Event Logs are utilized for logging kernel and user mode events. Security and low-level hardware events are also logged in Windows Event Logs. Therefore, understanding these logs is necessary for system administrators, cybersecurity professionals, and digital forensics practitioners.

B. Windows Event Logs:

Microsoft Windows provides a centralized logging mechanism that applications and the operating system can use to store their events. Windows provides an application called Event Viewer, which can be used to view these logs. Windows Event Viewer was introduced in Windows NT and has been part of all the versions of Windows since then.

Windows Event Logs typically contains the following information:

- Level – indicates the severity of the logged event. Following are the log levels available in Windows Event Logs:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

TABLE I. EVENT LEVEL

Log Level	Description
Verbose	Detailed output of the event log entry
Information	Generally used by applications and operating system components to denote successful execution of an operation
Warning	Not an error, but a possible source of issues in future
Error	Failure of an operation. It may indicate the source of a problem in an operating system service, component or application.
Critical	The major issue that should be addressed immediately.

The levels of event log entries are decided by the developers of the applications or services. The levels "Verbose" and "Information" generally contain informational messages such as successful completion of background tasks and so on. The levels, Warning, Error, and Critical are degrees of the criticality of failure cases.

- Date and Time: timestamp of the occurrence of an event.
- Source application or service that generated the event may include services or applications of the operating system.
- Event ID: a unique ID of the event being logged. The same ID is expected to be used in all the instances of the event being logged. For example, Event ID with a value of 4624 has a description "An account was successfully logged on."
- Task Category – applications that have generated the event, the "event source", can further categorize the event by giving the event a number and a text label. For example, events with ID 4624 have a task category "Logon". This field helps users of Windows Event Viewer to filter events.

Based on the type of the event and their source, event logs may store the following additional information [3]:

TABLE II. ADDITIONAL PARAMETERS OF WINDOWS EVENT LOG

Event Log Parameter	Description
Keywords associated with the event	They are text strings associated with an event. The developer of the application provides these strings.
User	The Windows user login associated with the event.
Operational Code	The internal code assigned by the application to the operation being performed when the event was logged
Log	Type of the log, typically Application, Security, etc.
Computer	Name of the computer
Thread ID	ID of the thread belonging to the process that generated the event
Process ID	ID of the process that generated the event
Session ID	Remote terminal session ID
Kernel Time	CPU time units utilized by kernel-mode instructions
User Time	CPU time units utilized by user-mode instructions
Processor Time	CPU ticks utilized by user-mode instructions
Correlation ID	It is the internal activity ID in the process that generated the event
Relative Correlation ID	It is related activity ID in the process that generated the event
Event Source Name	It is the name of the event source as specified by the application

As mentioned in TABLE II, one of the parameters stored in the Windows Event Log is called "Log". Windows Event Log uses this parameter to categorize the log entry like one of these:

- Application
- Security
- Setup
- System
- Forwarded Events

Application and Services category contains sub-categories such as:

- Hardware Events – events generated by the applications, components and services that access the hardware.
- Microsoft – logs of system applications and services
- Microsoft Office Alerts – events generated by Microsoft Office applications
- Key Management Service – events of Windows Key Management Services
- Logs of various other applications and services

Windows Event Viewer provides a consolidated front-end for all the categories of logs.

C. Windows Event Logs and their uses in Digital Forensics:

Windows Event Logs contain logs that are generated by events in applications and the operating system. These log entries can be correlated with user actions, such as user logins, time periods when the system was in use, applications used at various points of time, etc. [7].

It should be noted that Windows Event Logs do not contain details of actions performed by the user in applications. For example, applications typically do not store events, such as when the user last accessed a particular menu or a feature. To log such actions, applications maintain separate logs and those are not linked with Windows Event Logs.

Windows Event Logs typically contain low-level application or operating system events. Here are a few examples of events that are logged by the operating system:

- User login and logoff
- Application Crash

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

- Installation of a hardware device
- Installation of Windows components and services

As mentioned above, event log entries do not contain logs about the actions of users within the applications. However, investigators should attempt to relate actions performed by the user as noted in application logs with Windows Event Log entries. In some cases, when application logs are not available, event log entries such as the user's login time and so on can be used to associate the data created or transmitted from the computer during the user's active usage time. In essence, Windows Event Log entries can help an investigator substantiate their findings from other sources on the computer, such as application logs, files created by the applications, etc. Windows Event Logs are beneficial to associate actions performed by the user in the applications with operating system-level events such as login and logoff times.

II. ACCESSING WINDOWS EVENT VIEWER

All Windows systems have an in-built application called Event Viewer, a Windows Event Log framework component that allows access to event logs on the system [4].

On Windows machine, click on Start and type Event Viewer and click on Event Viewer. Once Event Viewer is launched, a window as shown in the Fig. 2.

The tree node on the left pane (Event Viewer) is the most important feature in Event Viewer as it helps navigate among different event logs.

When the "Custom Views" node is expanded, the options are displayed as shown in Fig. 3.

When Windows Logs are expanded, the logs are displayed as shown in Fig. 4.

When "Application and Services Logs" are expanded, the options are displayed as shown in Fig. 5.

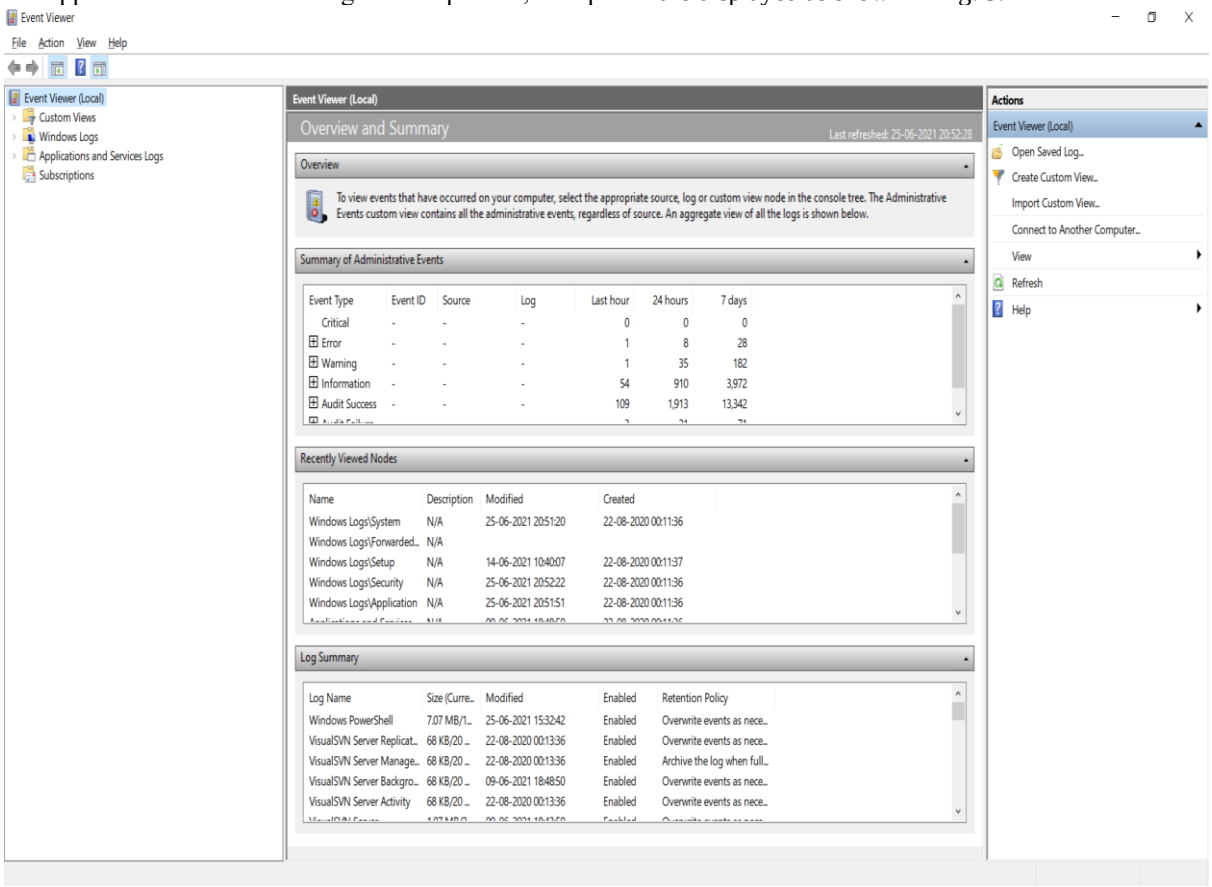

Fig. 2: Windows Event Viewer

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

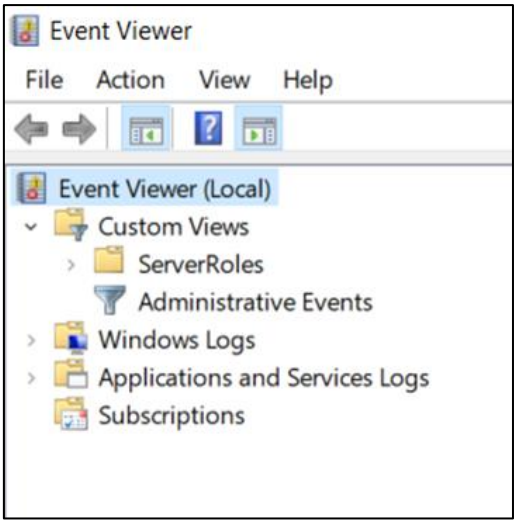

Fig. 3: Custom Views in Windows Event Viewer

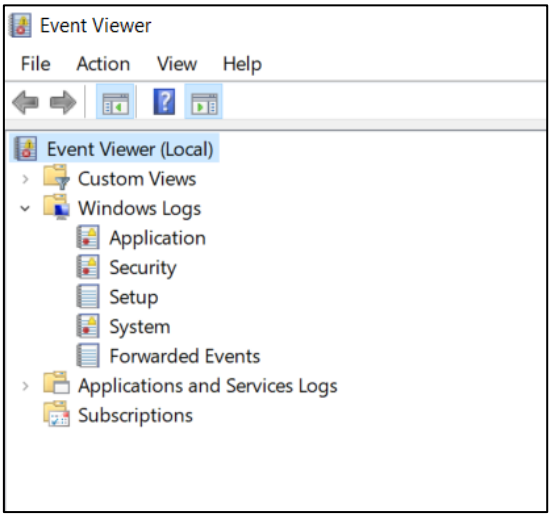

Fig. 4: Windows Event Logs

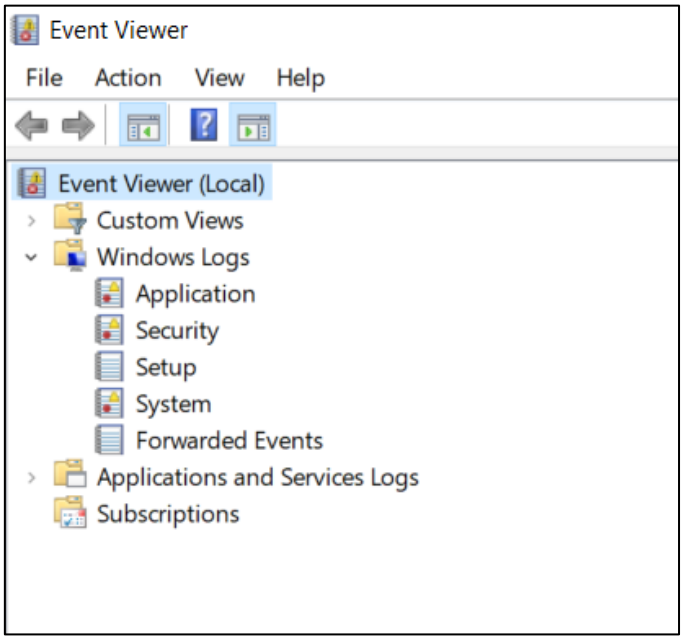

Fig. 5: Application and Service Logs

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Clicking on any of the above nodes would open the relevant log. Each log is displayed in a tabular structure, with each row representing an event. The following screenshot displays the contents of the Application log on a Windows machine:

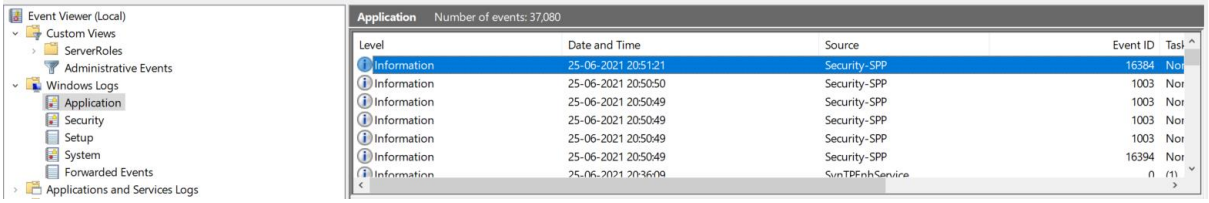

Fig. 6: Event Log Entries

Contents of other logs were also presented in a similar manner. As shown in the screenshot above, each row represents one event. Each column represents event data of a particular type, such as Event ID, Level, etc. The display columns can be customized by right-clicking on the table header and selecting the "Add/Remove Columns…" option.

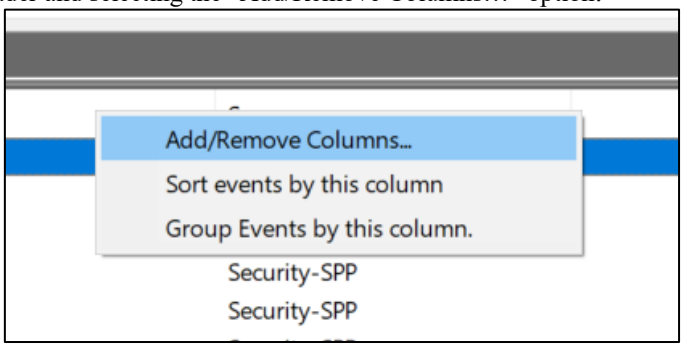

Fig. 7: Add/Remove Columns in Event Viewer

Clicking this option shows the following dialog box using which the user can customize the columns that can be displayed in the log entries table.

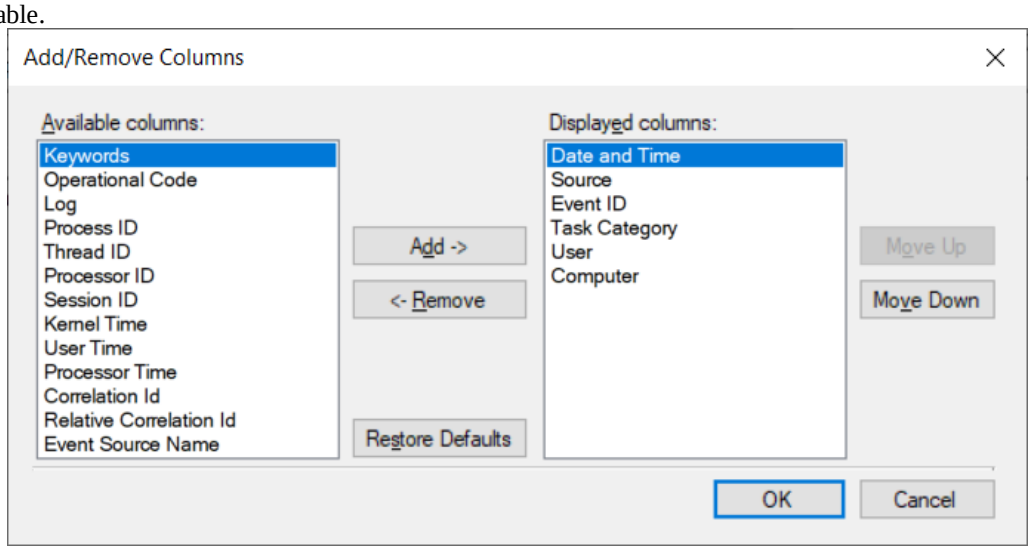

Fig. 8: Customizing Event Viewer

Note that columns should be customized for each log type (nodes on the left side such as Application, Security, Setup and so on).

Selecting a row in the events table displays details of the event in the bottom panel (as shown in Fig. 9).

Windows Event Viewer also provides the feature for an administrator to connect to a remote system (for which the administrator has access) and access its logs.

It is important to note that an investigator will most likely be using digital forensics software to explore the contents of event log entries. Digital forensics applications provide features to explore and search within event log entries. The mechanism described in this section is useful to explore and understand the contents of event log entries in a non-investigative scenario. Event log analysis should always be performed using digital forensics software to generate forensically acceptable reports.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

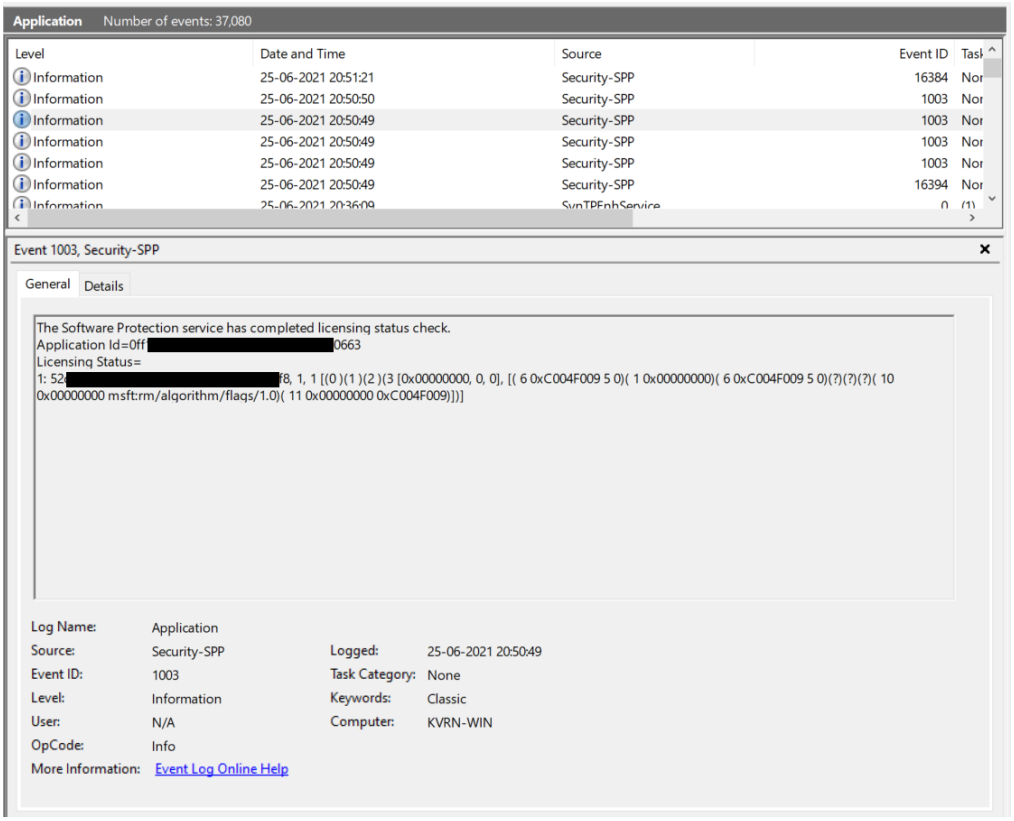

Fig. 9: Event Information

III. USE OF DIGITAL FORENSICS APPLICATIONS FOR EVENT LOG ANALYSIS

Digital forensics applications are connected to evidence disks using a write-blocker. A bitstream copy of the entire evidence disk is then taken and saved into a file. This file, which is called a disk image as a copy of the entire hard disk, contains all the hard disk contents. Digital forensics applications reconstruct the file system and its contents based on the data on the disk image. Event log files would also be available as part of the Windows installation folder. Digital forensics applications read and parse the raw event log files to reconstruct the structure of the logs and their events. Event log files are located at:

<Windows Installation Folder>\ System32\winevt\Logs

Most commonly, the location would be:

C:\Windows\System32\winevt\Logs

This folder contains many files with the extension “evtx”. Older versions of Windows had a different format with the extension “evt”. Windows operating system organizes event log entries among these files. These files are in binary formats and cannot be understood using text editors. Digital forensics applications can parse both the formats. Once the files are parsed, digital forensics applications present the entries in the log in a viewer similar to Windows Event Viewer.

Following is a shortlist of digital forensics applications that support analyzing contents of Windows Event Log files.

1. Autopsy (https://www.autopsy.com/)
2. Belkasoft (https://belkasoft.com/ec)
3. Encase (https://security.opentext.com/encase-forensic)
4. FTK (https://accessdata.com/products-services/forensic-toolkit-ftk)
5. Magnet Forensics (https://www.magnetforensics.com/)
6. ProDiscover (https://www.prodiscover.com/)

Each digital forensics product has its particular strengths and by no means a single tool can provide all the required features. Hence a digital forensics professional should explore and learn features in different products.

The following list is not technically digital forensics applications but provides features to explore and analyze Windows Event Logs:

1. LogParser (https://www.microsoft.com/en-in/download/details.aspx?id=24659)
2. Event Log Explorer (https://eventlogxp.com/)
3. LOGAlyze (https://sourceforge.net/software/product/LOGalyze/)
4. GrayLog (https://www.graylog.org/)
5. Event Log Check (https://documentation.n-able.com/remote-management/userguide/ Content/eventlogcheck.htm)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

IV. WINDOWS EVENT LOG ENTRIES OF INTEREST FOR INVESTIGATORS

Event IDs of logged events are unique and form the basis for an investigation. Details of events, such as event categories, keywords and operational codes, help in filtering events. Events are also tagged with the user and computer name. These properties are vital in linking an event with the logged-in user. The date and time of the event help in understanding the series of events that are linked to actions of particular applications and the operating system. Event source provides details of the application or operating system service that has logged the event. All these together will help in identifying events that are of value in the investigation.

Following are some of the important event IDs that can help in digital crime investigations [1]:

TABLE III. EVENT ID AND DESCRIPTIONS

Event ID	Description	Log Type
1	The system time has changed	System
19	Installation Successful – Windows update or Definition Update for Windows Defender completed successfully	System
20	Installation Error	System
42	The system is entering sleep (Sleep Reason: Button or Lid)	System
43	Installation Started – Windows Update or Definition Update for Windows Defender started	System
44	Windows Update Service started downloading an update	System
106	Task Scheduled	Windows Task Schedular (Operational)
200	Task Executed	Windows Task Schedular (Operational)
201	Task Completed	Windows Task Schedular (Operational)
141	Task Removed	Windows Task Schedular (Operational)
1100	Event logging service shutdown	Security
1102	Audit logs cleared	Security
1149	User successfully authenticated with remote desktop	Terminal Services
4000	Attempted to connected wireless network	System
4616	System time changed	Security
4624	Successful login	Security
4624	Login successful	Security
4626	Login failed	Security
4634	Successful logoff	Security
4648	Login attempted with explicit credentials	Security
4648	A logon attempted using credentials (could be remote access attempted)	Security
4688	A new process created	Security
4689	A process terminated	Security
4720	New user account created	Security
4722	User account enabled	Security
4723	A member added to security-enabled local group	Security
4724	User password reset	Security
4728	A member added to security-enabled global group	Security
4776	Attempted to validate credentials	Security
5140	Network share object accessed	Security
6005	Event log service started	System
6006	Event log service stopped	System
6008	Unexpected system shutdown	System
6013	System uptime	System
8194	Successfully created system restore	Application
8216	System Restore creation skipped	Application
8300	Scoping started for shadow copy	Application
8301	Scoping completed for shadow copy	Application
8302	Scoping successfully completed	Application

The above table represents Event IDs of operating-system-level events. Applications may add their specific events with their preferred ranges of Event IDs. Windows allows applications to add Event IDs from 0 to 65535. The documentation of applications should be consulted to understand their event log entries.

A. Limitations:

Microsoft primarily uses windows Event Logs to store log entries of Windows and some of its products such as Microsoft Office, SQL Server, etc. Most software applications do not use Windows Event Logs to store their log entries. Even in such cases, the operating system may also store some of the events pertaining to these applications, such as when a process associated with these applications is terminated, etc. The reasons for such events getting into the Windows Event Log are not directly apparent from the logs themselves. They may require further investigation elsewhere in the system, such as the file system entries, registry entries, application-specific logs, etc.

Investigators should note that event log entries may not contain all the parameters. For example, Kernel Time and User Time are not generally logged by applications and operating systems (that is, its applications and services).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 07, July-2021

Some events may not be logged by default and may require additional configuration to switch on logging of these events. For example, by default, Windows does not log events such as locking of the system. The absence of certain event log entries should not be treated as if the events have not taken place.

Another major challenge for an investigator is processing and analyzing a huge number of events that are being continuously logged [5].

Malware running on the computer can tamper with events in the event log. Users may also download utilities from the Internet that assist in deleting events. It is tough to identify such scenarios and may require advanced techniques to identify such actions.

V. CONCLUSION

Event log analysis is more of an art than science. The Event Logs are categorized into different categories such as application, system, and security with different levels of severity. Based on the nature of the investigation, event logs should be filtered, collated and then a timeline of events should be reconstructed. This timeline of events should then be used to correlate with entries in other areas of Windows, such as from the registry, startup actions, etc. This data can then be matched with discoveries made on the file system, such as MAC timestamps and deleted files, to have a complete picture of user actions on the computer. Event log analysis is one piece of the puzzle that should be solved and related to the rest of the evidence available on a computer to understand the user actions on the evidence system comprehensively. Windows Event Logs are also valuable for identifying possible unauthorized access. A thorough analysis of the Windows Event Log and reconstruction of events related to the investigation can strengthen the case [6].

As noted in this paper, Event IDs are available for operating system-level events [2]. Where applications are found to be using the Windows Event Log mechanism, Event IDs and related details of those applications should be obtained to analyze further and reach a logical end.

Windows Event Logs are essential from the digital forensic perspective as they store critical operating system and application events. Though Windows Event Logs have been part of the Windows operating system for more than two decades, their utility in digital forensics has been limited due to its complexity in analysis. A significant challenge is finding investigative value events and utilizing those events to correlate with other data on the computer. It requires an insight into the event log mechanism and significant experience that can only be gained with technical knowledge.

REFERENCES

[1] Webpage: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
[2] Webpage: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/
[3] WebPage: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc765981(v=ws.11)?redirectedfrom=MSDN
[4] Zeng, L., Xiao, Y., Chen, H., Sun, B., & Han, W. (2016). Computer operating system logging and security issues: a survey. Secure Communication Networks, 9, 4804-4821.
[5] J. Dwyer and T. M. Truta, "Finding anomalies in windows event logs using standard deviation," 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013, pp. 563-570, doi: 10.4108/icst.collaboratecom.2013.254136.
[6] Ibrahim N.M., Al-Nemrat A., Jahankhani H., Bashroush R. (2012) Sufficiency of Windows Event Log as Evidence in Digital Forensics. In: Georgiadis C.K., Jahankhani H., Pimenidis E., Bashroush R., Al-Nemrat A. (eds) Global Security, Safety and Sustainability & e-Democracy. e-Democracy 2011, ICGS3 2011. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 99. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33448-1_34
[7] Dashora, K., Tomar, D.S. and Rana, J.L. (2010) A practical approach to evidence gathering in Windows environment, 5 (8), pp.21-27