**BACKGROUND AND MOTIVATION**

Windows Event Logs provide wealth of information for system monitoring, troubleshooting, security, compliance, performance analysis, and more. Leveraging these logs effectively can improve system reliability, enhance security, optimize performance, and streamline IT operations. However, working with Windows Event Logs can pose many challenges. For example; log volume and scalability, log collection, management, storage and Retention; log filtering, parsing, analysis and correlation; log monitoring, alerting, security and integrity; log compatibility, versioning and performance impact; understanding logs and interpreting them.

**PROBLEM**

How can Windows Event log data be analyzed and visualized in a manner that is interactive and intuitive for system administrators?

**AIMS**

The primary aims of this project are to work with a Windows Event Log data set and to create way for prospective system administrators to:

* Interactively query event logs
* Visualize event logs.
* Identify correlations in the event log dataset.

**OBJECTIVES**

* Research existing windows event log tools for working with Windows Event Logs.
* Research techniques for preparing, structuring, managing Windows Event Log raw data.
* Design an artefact that can be used for interaction with Windows Event Log data.
* Acquire resources and deploy the architecture for the artefact.
* Implement the artefact.
* Test the artefact with users.
* Capture and interpret results from testing.

**RESEARCH QUESTIONS:**

1. What are the best ways to organise and prepare raw Windows Event Log data so that analysis and visualisation can be done quickly and effectively?
2. How to compare the capabilities and usability of several Windows Event Log solutions for interactive querying and visualization?
3. What relationships and patterns may be found in datasets of Windows Event Logs, and how can these relationships be used to comprehend system behaviour and possible security incidents?

# Literature review:

Forensic investigations involve log investigation because it tends to make investigation relatively easy and accelerates security. Logs provide important information about the intruder activities which could be involved in hacking of systems and website, DOS attack. Audit logs are very complicated log events and format is in binary form. Moreover, windows log events are decentralized in nature. To cope with these complexities and emphasize the importance over In this study [1], The author recommends a reasonable alternative for decentralized log storage which then seems to be using Win Syslog which is a central Syslog server and event reporter that can translate the data into syslog format from the binary format.

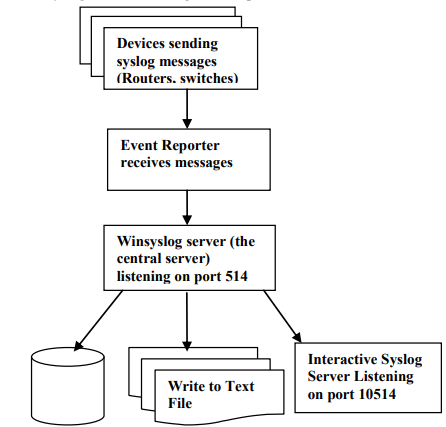


Figure 1: Different sources of logs collecting in Winsyslog [1]

Further study concludes that [2], Cybercrime is growing ever more relatively common, thereby further it needs to be evidence already when individuals may very well be accused of violating the law. Scientific proof, legal requirements, and Windows OS source materials as well as the Tracking system, slack space, and event log seem to be the major talking points of this research project. A VMware computer system was utilized to simulate cybercrime operational processes the same as computer-controlled password guessing and getting hacked on such a Windows operating system. Event information and data have been thoroughly investigated for weight and social acceptance by windows log investigation.

In this study the author concludes that [3], the Windows event log is a flawed tool used in digital forensic cases, often not being considered verifiable. This dissertation aims to develop a solution to address flaws in the Windows event logging service. Research found that disabling the service allowed for modification of important data and easy transplantation of event logs. A C# and Microsoft.NET-based event logging application was developed, using RSA and AES encryption and HMAC hash signatures to improve data integrity. The application consists of an event logger, an event viewer, and a symmetric and asymmetric encryption. The symmetric encryption was found to be 800% faster than asymmetric encryption, and the HMAC hash signatures were tested for brute force attacks.

In this approach [4], A Windows event forensic entire process is explained in this article (Win EFP) to try and understand the event log files with the Windows operating system. The Win EFP deals with forensics of logs of activities and occurrences that take place in Windows. As a consequence, it aims to provide guidance to forensic investigators on continuing to investigate digital forensics via Windows event logs. Including both business and home environments, Windows happens to be the most widely utilized operating system. The Windows event forensic service expects that the event logging service is not clear and unambiguously ended up turning off by a Windows user. Win EFP could be employed in almost any forensic official investigation. that included a computer windows XP. Many Windows event log items that used to be extremely important for forensics were catalogued and identified in process of WinEFP development.

The proposed theory states that [5] logs contain a great deal of runtime information; logs are essential to the design and administration of software development system. As the complexity and size of software are increasing, the volume of logs are also increasing. As there is a shortage of openly accessible data sets and standardization, so only a small proportion of AI-powered log analytics techniques have already been successfully implemented in the sector over the past several years. Log hub had also managed to gather 17 real-world log datasets from those of a wide range of technologies, which include supercomputers, distributed systems, mobile systems, operating systems, server applications, and dedicated software. The paper also provides a situational analysis on intrusion detection system, describes the data, and introduces real-world usage specific cases. Including around 77 GB of data, Log hub is a 17-log dataset enabling log analytics that uses artificial intelligence. It supports the log activities of the organization and continues to act as a discussion board for performance monitoring, datasets, and comments from business and the academic community. Log hub has indeed been downloaded by over 380 organizations, and the platform is planning on keeping trying to gather clearly labelled datasets and planning to release open-source log analysis toolkits.

## **Technology and tools**

1. **Window event viewer for log visualization and query**

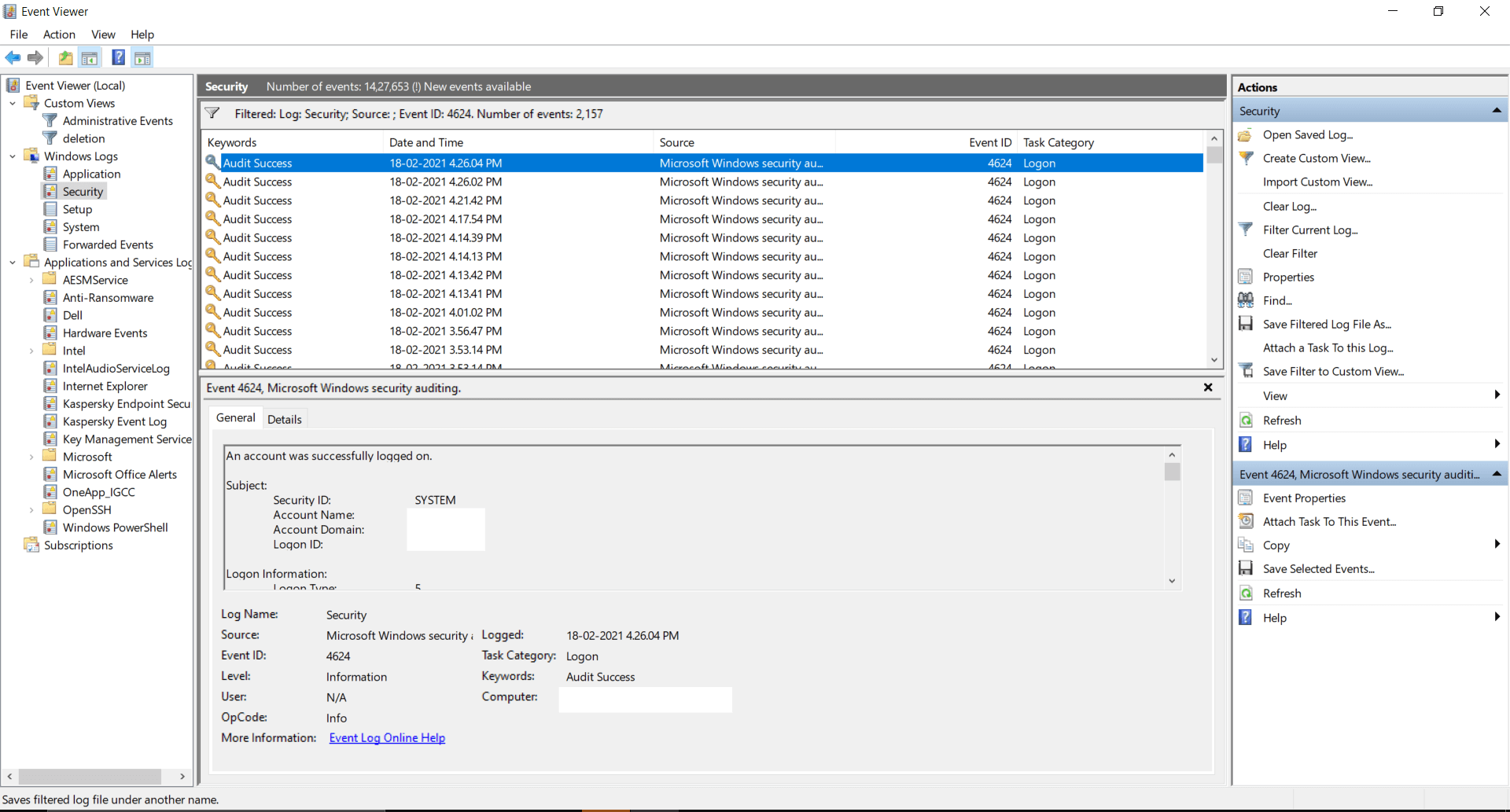
The Windows Event Viewer is a dynamic tool which administer query log events and visualization for event logs in the Windows operating system. Furthermore, it also grants users the opportunity to analyze and view numerous event logs, as well as authorize advanced querying to refine and search for events that are based on numerous criteria.

To employ the Windows Event Viewer for log visualization and querying:

* Firstly, open Event Viewer: Press the Windows key + R, for the opening of the Run dialog box, type "EVENTVWR.MSC", and press Enter. This will open the Event Viewer application.
* operate to Event Logs: In the Event Viewer window, you will be able to find wide range of event log folders on the left-hand side, that includes security, application, System, and others. Click on the significant log folder to view its recorded events.
* View Events: Clicking on a log folder will display the recorded events in the main pane on the right. You can scroll through the events to examine their details.
* Filter Events: To perform a basic filter, click "Filter Current Log" in the Actions pane on the right. You will be able to filter events by different parameters like keywords, event IDs, event source, as well as date ranges.
* Create Custom Queries: For more up-to-date querying, use the "Create Custom View" option in the Actions pane. This will grant you the ability to build complex queries that are based on specific criteria, such as keywords, event IDs, event sources, event levels, and others.
* Save Queries: user can save custom queries for the future use and easy access.

Through employing the query capabilities and log visualization of the Windows Event Viewer, operators will be efficiently analyzing event logs, monitor system performance, troubleshoot issues, further investigate security incidents, ultimately helping to maintain the security and health of the Windows environment.

it is necessary to have “security information and event management” (SIEM), this solution not only aggregate the logs rather they also provide user to efficiently visualize the data and gather evaluative perception. The old method of analyzing the logs is:



**Features of event log analyzer**

* SEIM
* IT compliance management
* Reporting console
* Log management
* File integrity monitoring
* Log forensic analysis.

1. **NirSoft utilities for log visualization and query**

NirSoft provides several tools for system troubleshooting, security, and maintenance. They would not provide a specific tool allocated entirely to querying and log visualization like Windows Event Viewer**.** Nevertheless, NirSoft's assemblage of services includes diverse tools that can be helpful for accessing and analyzing defined types of logs on Windows systems. For example:

* Nir-Soft's "Event Log Sources View" service allows the user to view a list of all event log sources equipped on your system, that also provides data and information related to each source as well as their associated event logs.
* "My Event Viewer" is another Nir-Soft tool. This tool presents a more user-friendly terminal than the default Event Viewer, authorizing the user to view event logs in an uncultured manner.
* "Last Activity View" presents an inclusive report on various system activities, such as user login, system shutdowns, and application installations. which can be handful for monitoring system troubleshooting and usage.

On other hand, While NirSoft activities offer beneficial performance for system analysis, they might not be able to cover the entire range of characteristics enabled by the local Windows Event Viewer. In case the user needs more up-to-date log visualization capabilities and querying, it is better to count on the local Event Viewer tool or investigate other functional log analysis tools that are available in the market.

1. **Splunk for windows log visualization and query**

Splunk is the most powerful log management system and analysis platform and an internationally well-known system, which can be utilized for querying and log visualization and includes window log data. It proposes indexing, application logs, hefty abilities for ingesting, system logs, examining log data from different sources, security logs, and window event logs and more.

* **Advanced querying**: Splunk’s search processing language (SPL), offers the user the chance to search on the log data and perform complex queries. Users can correspond and filtrate, and analyze the time range, event types and as well as keywords.
* **Data visualization:** Splunk enables a user-friendly affiliate to generate interactive visualization and dashboards. Through log data, users can generate tables, maps, graphs, and charts to gather insights.
* **Indexing and parsing**: Splunk indexes and parses the log data to make it easy to search for the user as well as enabling efficient and fast querying after ingestion.
* **Data ingestion:** By using different methods like window event log monitoring, Splunk universal forwarder, or HTTP event collector, Splunk allows the users to ingest the data from the window machines.
* **Reporting and analytics:** to initialize the analytic based on log data and custom reports, Splunk proposes the reporting characteristic. These can be scheduled for distribution and automatic generation.
* **Alerting and monitoring:** based on the custom searches and already defined conditions, Splunk allows users to set up notification and alerts.

**METHODOLOGY:**

Project management for this project involves:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Project Initiation** | **Task Identification and Planning** | **Execution** | **Project Review and Evaluation** | **Documentation** |
| Define the project scope | Establish the schedule of project with start date and the end dates | Comparing the different tools and select the one tool to work with artefact | Project should be reviewed against defined aims and objectives | Project documentation includes design and plan of artefact and write-up of report |
| expected outcomes | Literature Review and technology review | Plan the artefact and work on it | Evaluate the artifact |  |

**RESULTS:**

Assess the artefact with other Windows Event Log tools that are already available, such Splunk, ELK Stack, and Grafana. Consider its advantages and disadvantages in terms of features, simplicity of use, and resource use.

Accuracy of Correlation Identification: Determine if the artefact can correctly find patterns and correlations in the event log dataset. This may entail confirming the veracity of the artefact's findings using well-known datasets with predetermined relationships.

Security Assessment: To verify that the artefact manages event log data safely and safeguards sensitive information, do a security review. Check to see whether access controls are being used properly.

Review of the documentation: Check the accuracy and clarity of the user manuals, installation manuals, and troubleshooting guides that are included with the artefact.

# **Reference**

[1] Sahoo, P.K., Chottray, R.K. and Pattnaiak, S., 2012. Research issues on windows event log. *International Journal of Computer Applications*, *41*(19).

[2] Ibrahim, N.M., Al-Nemrat, A., Jahankhani, H. and Bashroush, R., 2011, August. Sufficiency of windows event log as evidence in digital forensics. In *International Conference on e-Democracy* (pp. 253-262). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Codona, B., 2007. Analysis and Evaluation of the Windows Event Log for Forensic Purposes. In *Honour Project, Edinburgh Napier Univ.*

[4] Do, Q., Martini, B., Looi, J., Wang, Y. and Choo, K.K., 2014. Windows event forensic process. In *Advances in Digital Forensics X: 10th IFIP WG 11.9 International Conference, Vienna, Austria, January 8-10, 2014, Revised Selected Papers 10* (pp. 87-100). Springer Berlin Heidelberg.

[5] He, S., Zhu, J., He, P. and Lyu, M.R., 2020. Loghub: A large collection of system log datasets towards automated log analytics. *arXiv preprint arXiv:2008.06448*.