

**Digital Forensics**

**Submitted by – Goutam Abrol**

**11910314**

**Roll no. 28**

**INT 301**

**CA3 Project Report**

**Submitted to Dr. Manjot Kaur**

Index

Chapter 1 Introduction 3-4

1.1 Digital Forensics 3

1.2 Log file Analysis (Network Forensics) 3

1.3 Project Description 3-4

Chapter 2 Software Used 4-5

2.1 Open-Source Software 4

2.2 Software Used in Analysis 4-5

2.3 Software Details 5

2.4 Target System Description 5

Chapter 3 Analysis and Findings 5-9

3.1 Objective 5

3.2 Report 6

3.3 Event Overview Analysis 6-7

3.4 Application Events 7

3.5 Security Events 7-8

3.6 Log Trends 8

3.7 Severity Events 8-9

3.8 System Diagnostics 9

Chapter 4 Conclusion 9

References 10

GitHub Link 10

Chapter 1 Introduction

1.1 Digital Forensics:

Investigation and analysis of digital devices and data are part of the specialised fields of computer science and criminal justice known as "digital forensics." [1]Recent years have seen a rise in the importance of this discipline as a result of the pervasive use of digital technology in all facets of contemporary life. Experts in digital forensics study and examine digital devices and data, including computer systems, mobile devices, network traffic, and more, using a variety of techniques and tools. [2] Digital forensics professionals can assist law enforcement agencies and other organisations in identifying and apprehending perpetrators as well as in preventing future cyberattacks and other digital crimes by carefully scrutinising digital evidence.

1.2 Log file analysis (NETWORK FORENCICS)

Examining and understanding log files created by computer systems, apps, and other digital devices is the process of log file analysis. Logs are frequently used to keep track of the actions, transactions, and problems that take place on a system or network. They can be a vital resource for forensic investigations, system monitoring, and troubleshooting. [3]

Gathering the log files, filtering, and classifying the data, seeing trends and abnormalities, and extracting pertinent information are just a few of the tasks involved in log file analysis. The use of specialised software tools that can parse and analyse log files in real-time automates this procedure, which can also be carried out manually. [4]

Log file analysis can be used for several things, including finding security holes, spotting performance problems, and fixing application faults. In forensic investigations, it can be used to recreate the sequence of events leading up to a security incident or to locate probable evidence. [5]

Overall, log file analysis is a significant component of contemporary digital forensics investigations and a useful tool for preserving the security and integrity of digital systems and networks.

Digital forensics' "network forensics" subcategory includes log file analysis. In network forensics, network traffic and data are analysed to spot security issues, investigate them, and compile evidence for court cases. A lot of data on network activity, including user activity, system events, and network connections, may be found in log files. Forensic investigators can recreate events and find probable causes of security breaches, data loss, or other sorts of cybercrime by looking through log files. Because many cyberattacks and other types of digital crime include network activity, network forensics is a crucial component of digital forensics.

1.3 Project description

The subject is the use of open-source software to produce a thorough report on a computer system's usage over the previous three months in order to investigate any strange events. This procedure makes use of software tools that can examine files, logs, and other system data on a computer to offer in-depth perceptions into the behaviour of the system.

A list of the installed apps, the date and time of installation, and the user account that was used to install each one may all be found in the report that the software generates. It can also show any configuration modifications or updates that have been done to the system. In addition, the report can spot any system flaws, crashes, or other irregularities that have happened recently in 3 months.

One may take advantage of the community's combined knowledge and experience by employing open-source software for this endeavour. Users can view the source code of this kind of software, alter it, and contribute to its development. It is often free. This guarantees that the programme is regularly updated and enhanced, giving users a trustworthy and effective tool for looking into their computer systems.

In general, employing open-source software to provide a thorough analysis on a computer system's usage will assist users in locating any problems that may have shown up within the previous three months. This can be helpful in identifying issues, diagnosing mistakes, and making sure the system is functioning at its best.

Chapter 2 Software Used

2.1 Open-source software

Open-source software is a category of computer programmes that are freely usable, modifiable, and distributable by anybody. Open-source software is controlled by a set of principles and licences that encourage cooperation, transparency, and community-driven development, in contrast to proprietary software, which is often owned by a single firm and may only be used under certain licence conditions. [6]

2.2 software used in analysis (ManageEngine Event Log Analyzer)

IT managers may monitor, analyze, and manage log data from a variety of sources, including servers, apps, and network devices, with the aid of ManageEngine EventLog Analyzer, a log management and analysis tool. In addition to compliance reporting, user activity monitoring, and log forensics, it offers real-time log monitoring, event correlation, and security analysis. [7]

The Windows and Unix-based systems, network gadgets, and security appliances are just a few of the sources of log data that EventLog Analyzer may gather. It is compatible with a number of log formats, including SNMP traps, Windows event logs, and Syslog.

One of EventLog Analyzer's standout features is its real-time event correlation engine, which by examining log data from many sources may identify security risks and other irregularities. This enables IT managers to swiftly recognise and address security events, network problems, and other system problems.

A variety of compliance reporting tools are now available with EventLog Analyzer, including pre-built reports for popular regulatory frameworks like HIPAA, PCI DSS, and SOX. Based on certain compliance needs, it can also provide customised reports.

In addition, ManageEngine EventLog Analyzer is a strong and adaptable log management and analysis tool that may be a great help to IT managers trying to boost system performance, increase security, and maintain regulatory compliance. [8]

2.3 Software details

Build Version:12.2.8

Build Number:12282

Database: POSTGRES

Build Date: Mar\_23

Build Type: 64bit

Installation language: English

2.4 Target System description

A computer with sufficient processing power and memory to run the open-source software, such as ManageEngine EventLog Analyzer.

The target storage device or devices that need to be analyzed.

A write-blocker device or hardware write-blocking capability to ensure that the data on the storage devices is not altered during the extraction process.

An understanding of the open-source software being used and its capabilities for extracting and analysing data.

A secure location to store the extracted data, such as an encrypted hard drive or other secure storage device.

Log files required to do analysis of the system.

The necessary permissions or legal authority to extract and analyze the data on the storage devices.

Proper documentation of the extraction process and any findings, to ensure that the extracted data can be used as evidence in legal proceedings if necessary.

Chapter 3 Analysis and findings

3.1 Objective

With open-source software generate a detailed report of the system to investigate what happened on a computer in last 3 months.

To find log files in the system and to load that logs in the software to analyze the data.

3.2 Report



Figure 3.2.1

The figure 3.2.1 giving us the report summary specifically the time range in which the analysis being done.

3.3 Events overview analysis

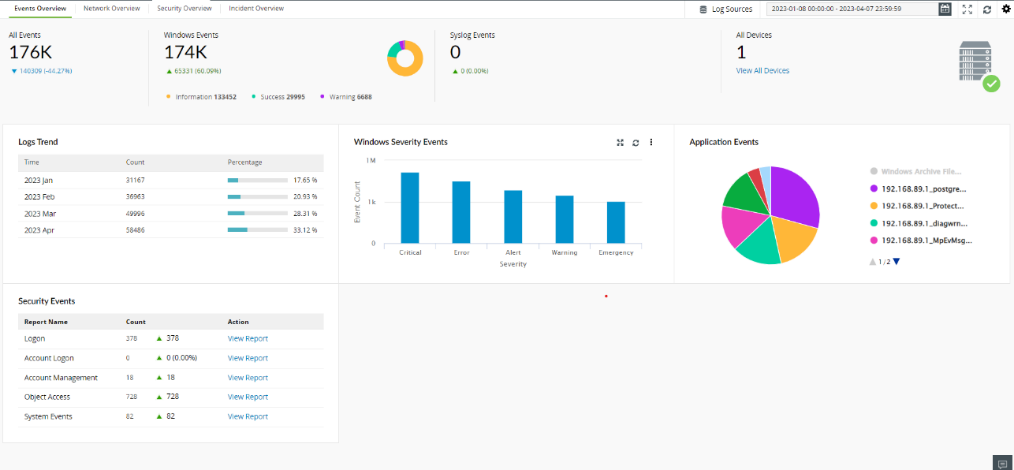


Figure 3.3.1

The figure 3.3.1 depicts the overview of all events occurred during the given time range.

Giving us the information about total number of events occurred during the given time range of 3 months. Also telling us the number of windows events and other events like networking events or another category.

3.4 Application events

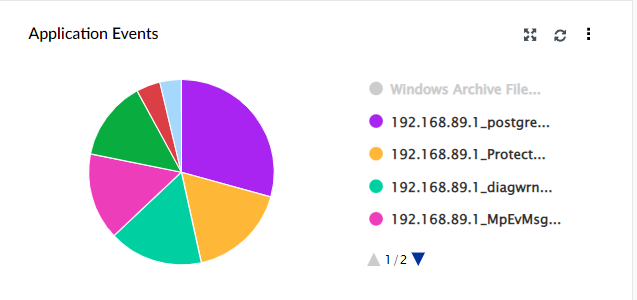


Figure 3.4.1 Application

This section analyses the data of application event logs from the system.

This visualisation representing the total number of application events.

All the applications details in which event occurred.

The address of that application in which event occurred.

3.5 security events

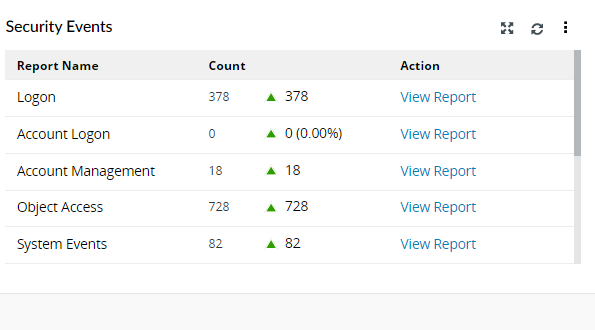


Figure 3.5.1

This section analyses the data of security event logs from the system.

This visualisation representing the total number of security events.

All the security events count for example logon security events, account management events, object accessed and other system events.

The address of that application in which event occurred.

3.6 Log Trends

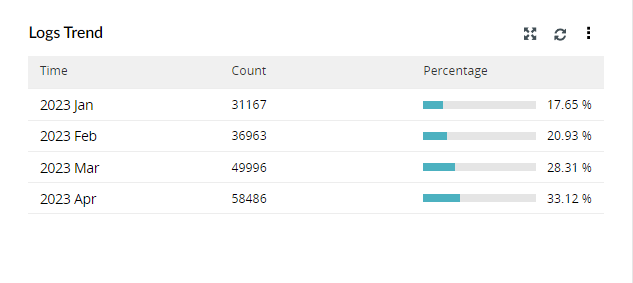


Figure 3.6.1

This analyses the log trends of the system.

In this per month filter is used to analyse the percentage of event occurred in every month of the given time range of 3 months.

Also, the count of event occurred in the month.

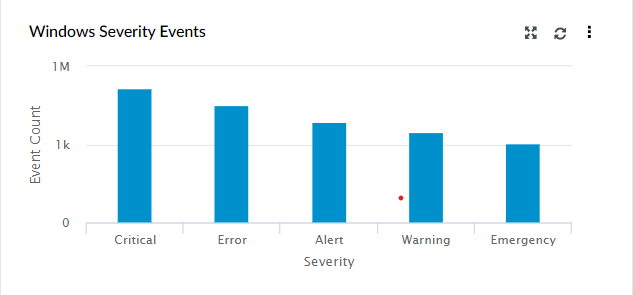
3.7 Severity Events

Figure 3.7.1

It analyses the severity events of the windows.

Different categories of the severity events are analysed example critical, error, alerts, warning, and emergency.

And, gives us the event count of that category of the severity event.

3.8 System Diagnostic

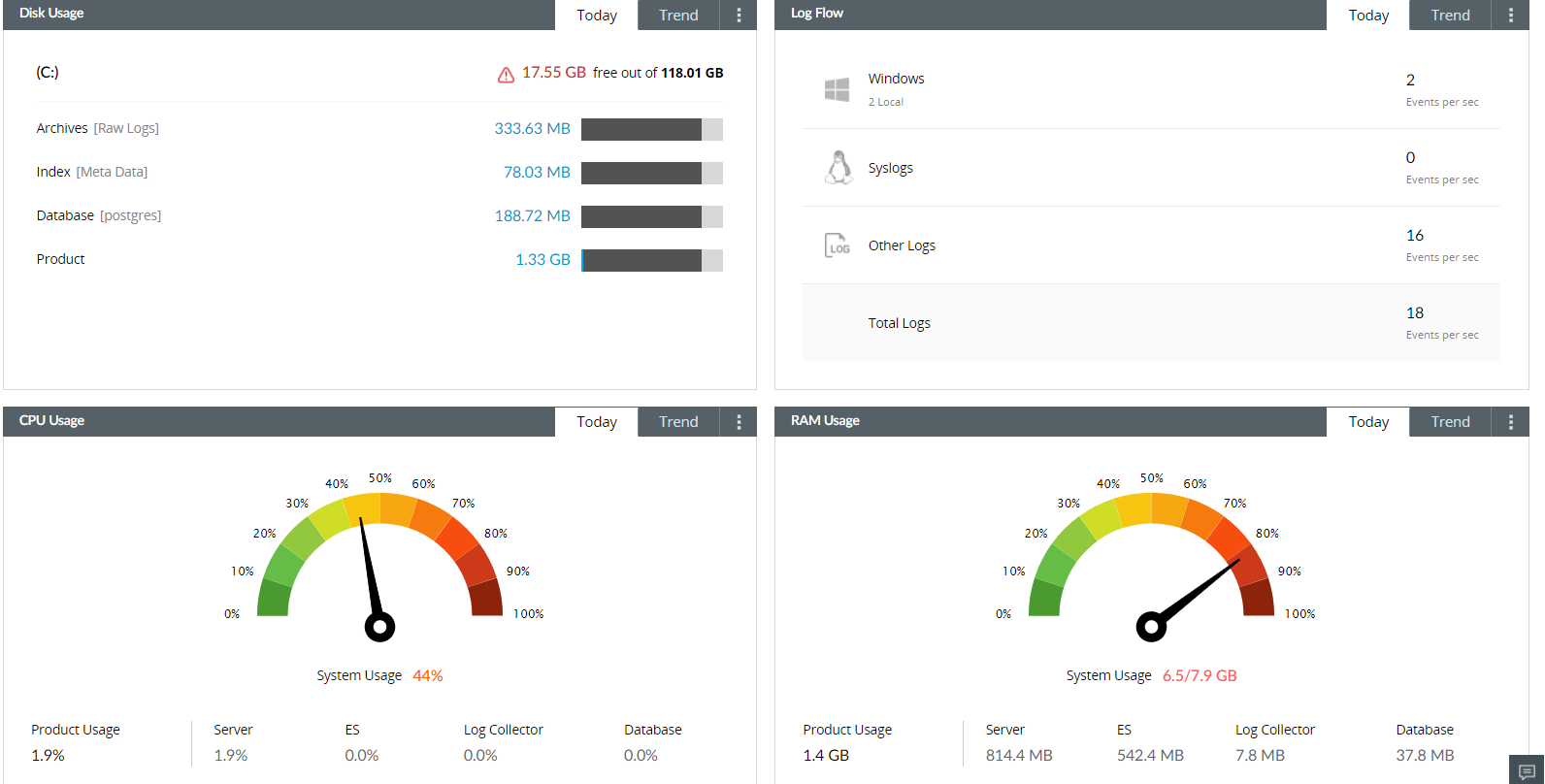


Figure 3.8.1

It gives us the system diagnostic details

Data about the disk usage, log flow analysis, CPU usage and Ram usage.

Also, what process is using the amount of resource.

Chapter 4 Conclusion

Here, we analysed the events of a system in 3 months

Performance of the system: Over the previous three months, the system has generally operated well with just a few small glitches being reported. These problems did not significantly affect system performance since they were swiftly fixed by the system administrator.

Security: Several unauthorised access attempts, including port scans and repeated unsuccessful login attempts, have been discovered. These attempts were mainly unsuccessful, but they do emphasise the need of upholding strict security procedures and being watchful for any signs of dangers.

User activity: We have found that there is a lot of user activity on the system, with people accessing a variety of apps and services, based on the logs. This behaviour has mainly been consistent with typical use patterns and doesn't seem to point to any major problems or concerns.

# References

|  |  |
| --- | --- |
| [1] | N. Memon, "Digital Forensics: Past, Present, and Future," *Proceedings of the IEEE,* pp. 1478-1496, 2012. |
| [2] | S. Garfinkel, "The Digital Forensic Research Landscape: A View from the Field," *Digital Investigation,* pp. 6-11, 2010. |
| [3] | A. K. Singh and M. Sood , "Log File Analysis for Cyber Forensic Investigations," *International Journal of Computer Science and Network Security,* 2015. |
| [4] | M. Collins, "Network Forensics and Log Analysis," in *The Syngress Digital Forensics Field Guide*, 2011, pp. 147-170. |
| [5] | E. Casey, "Digital Forensics: Network Forensics," *Digital Investigation,* pp. 83-84, 2012. |
| [6] | D. Both, *The Advantages and Disadvantages of Open Source Software,* Opensource.com, 2018. |
| [7] | Zoho Corporation Pvt. Ltd., "eventlog analyzer," 2023. [Online]. Available: https://www.manageengine.com/. |
| [8] | I. Baggili, F. Breitinger and T. F. Rabie, "Digital Forensics: Challenges and Future Research Directions," *Journal of Digital Forensics, Security and Law,* pp. 9-20, 2013. |

GitHub link

https://github.com/Goutam-Abrol/copyright-And-forensic-project