Git Hub Link- https://github.com/aryan098-max/Int301CA

Registration Number – 11914145, Roll Number – 28

Question - Use any open-source software to generate a detailed report of your system to investigate what happened on a computer in last 3 months.

1. Introduction:

Logwatch is an open-source log analysis and reporting tool that helps administrators monitor their systems and identify potential issues quickly and easily. It automates the log analysis process and provides an easy-to-read summary of system logs, which can be customized to focus on specific areas of interest. The tool can be configured to run on a regular schedule, such as daily or weekly, and can send the report to an email address or save it to a file. Logwatch is widely used in the Linux community and can be integrated with other monitoring tools to provide a more comprehensive view of system activity. Overall, Logwatch is a valuable addition to any system administrator's toolkit.

1.1 Objective of the project:

The objective of generating a detailed report using an open-source software is to gain insights into a system's activity over the last three months. This can help identify potential issues or security threats, understand user behaviour, and improve system performance. By using open-source software, users can access a wide range of tools and resources without paying for proprietary solutions, which can be beneficial for organizations or individuals with limited budgets. The report generated by analysing various system logs provides insights into user logins, file modifications, network activity, system errors, and other system events, helping to improve the system's security, reliability, and performance.

1.2 Description of the project:

The project aims to generate a detailed report of a computer system's activity over the last three months using any open-source software. The objective is to gain insights into potential issues, security threats, user behaviour, and system performance. By analysing various system logs, the report can be customized to focus on specific areas of interest and provide a better understanding of the system's overall health. Using open-source software allows access to a wide range of tools and resources without having to pay for proprietary solutions, making it particularly beneficial for organizations or individuals with limited budgets. Ultimately, the project aims to improve the system's security, reliability, and performance by providing insights into its activity.

1.3 Scope of the project:

The scope of the project is to use open-source software to generate a detailed report of a computer system's activity over the last three months. The project involves capturing and analysing various system logs and can be customized to focus on specific areas of interest. The report can be scheduled to run regularly and can be sent to an email address or saved to a file. The project's scope is to provide insights into potential issues, security threats, user behaviour, and system performance. It is designed as a reporting tool for system administrators to make informed decisions and take appropriate actions based on the insights gained from the generated report.

2. System Description:

Device name: LAPTOP-S7MB25C9

Processor: Intel(R) Core (TM) i5-1035G1 CPU @ 1.00GHz 1.19 GHz

Installed RAM: 8.00 GB (7.78 GB usable)

Device ID: D6F2EF23-16C7-42E6-9EDF-1FB588C9E691

Product ID: 00327-35194-34182-AAOEM

System type: 64-bit operating system, x64-based processor

2.1 Target system description:

The target system is a laptop with a device name LAPTOP-S7MB25C9, its processor is Intel(R) Core (TM) i5-1035G1 CPU @ 1.00GHz 1.19 GHz, it's device id and product id is D6F2EF23-16C7-42E6-9EDF-1FB588C9E691 and 00327-35194-34182-AAOEM respectively. A total of 8 GB ram is installed inside the system and its type is 64-bit operating system, x64-bases processor.

2.2 Assumptions and Dependencies:

The assumptions and dependencies for generating a detailed report of the target system's activity over the last three months using an open-source software -

1.Assumptions:

- The system has been running without any major issues that may have affected the accuracy or completeness of the system logs.
- The necessary system logs required to generate the report have been enabled and are being recorded.
- The open-source software selected for generating the report is compatible with the target system's operating system and hardware.

2.Dependencies:

- Access to the system and its logs is required to generate the report.
- Sufficient storage space may be required to store the logs and the generated report.
- The open-source software selected for generating the report must be installed and properly configured on the system.
- Knowledge and expertise in using the selected open-source software is necessary to generate a comprehensive report.

2.3 Functional and Non-Functional Dependencies

1.Function Dependencies:

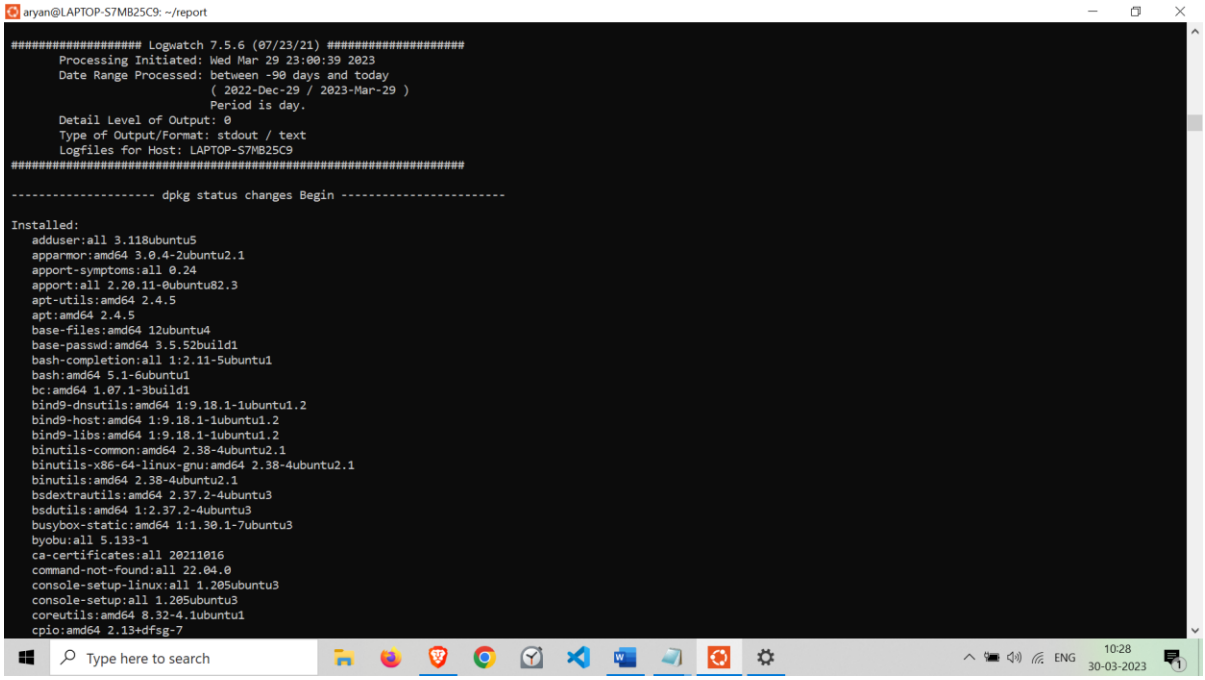
- The availability of logs containing information on the system's activity over the last three months is necessary to generate the report.
- The selected open-source software must be capable of capturing and analysing the logs to generate a comprehensive report.

2.Non-Functional Dependencies:

- The speed of the system and its storage capacity may affect the time taken to generate the report.
- The accuracy and completeness of the report may depend on the quality and quantity of the logs captured.
- The selected open-source software must be reliable and efficient in generating the report.
- Security of the logs and generated report must be maintained to prevent unauthorized access or tampering.

2.4 Data set used in support of your project.

The dataset in this project would be the log that has been generated by the system.

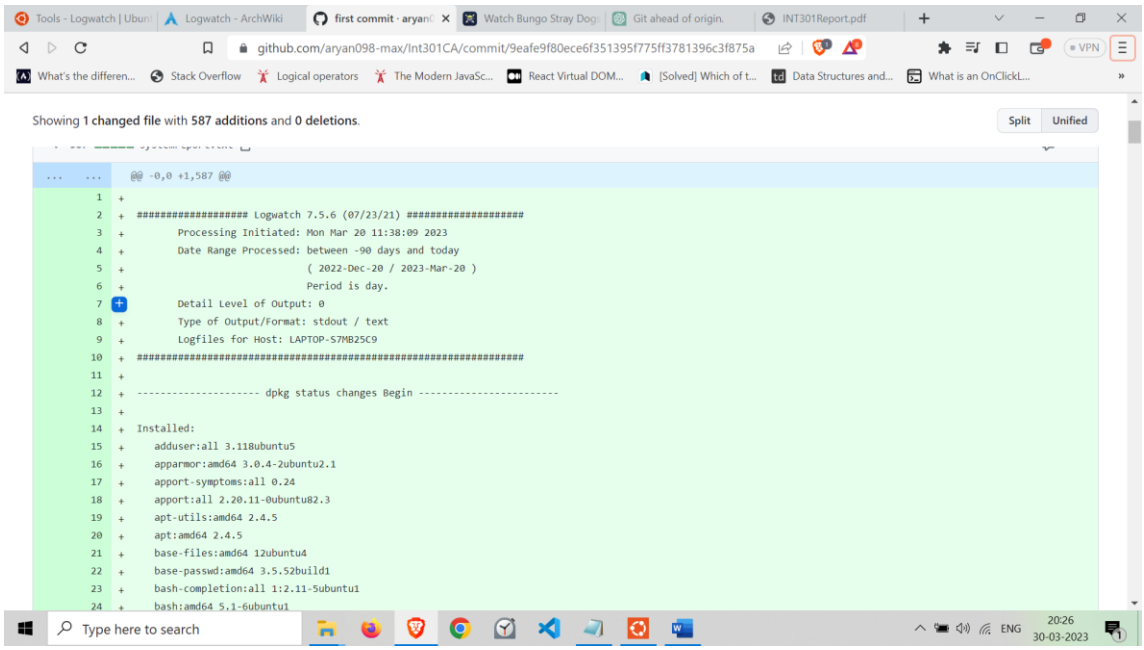


3. Analysis Report

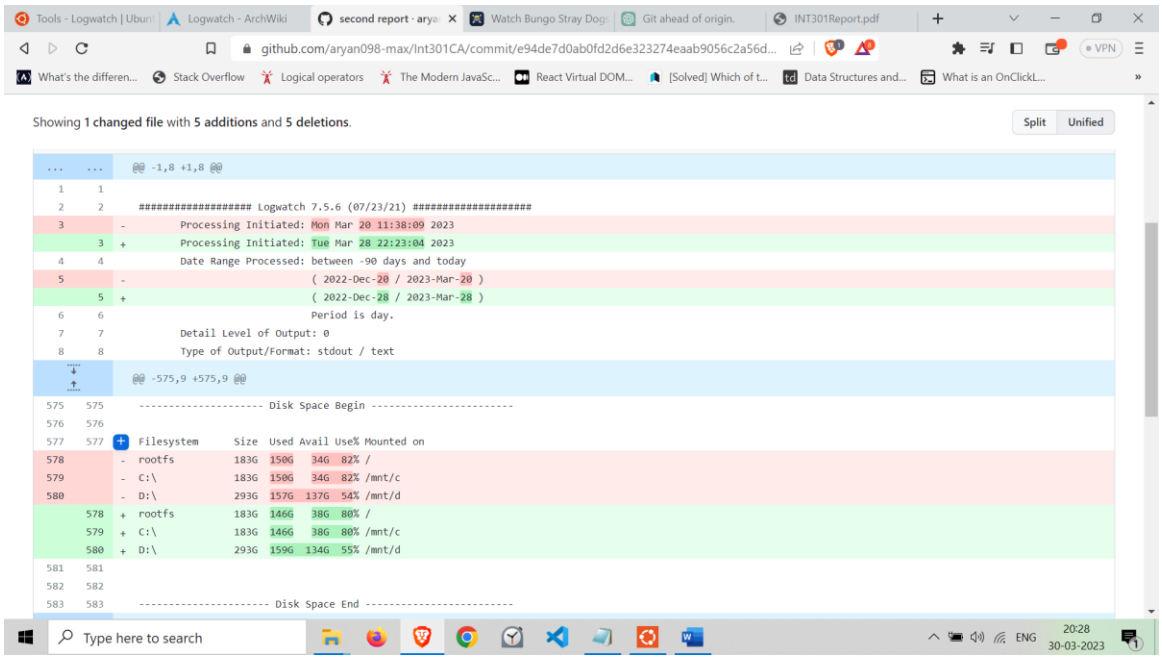
The analysis report of this project would be summery of the system activity, User activity, File activity, network activity, system errors, security threats that has happened in the last three months.

3.1 System snapshots and full analysis report

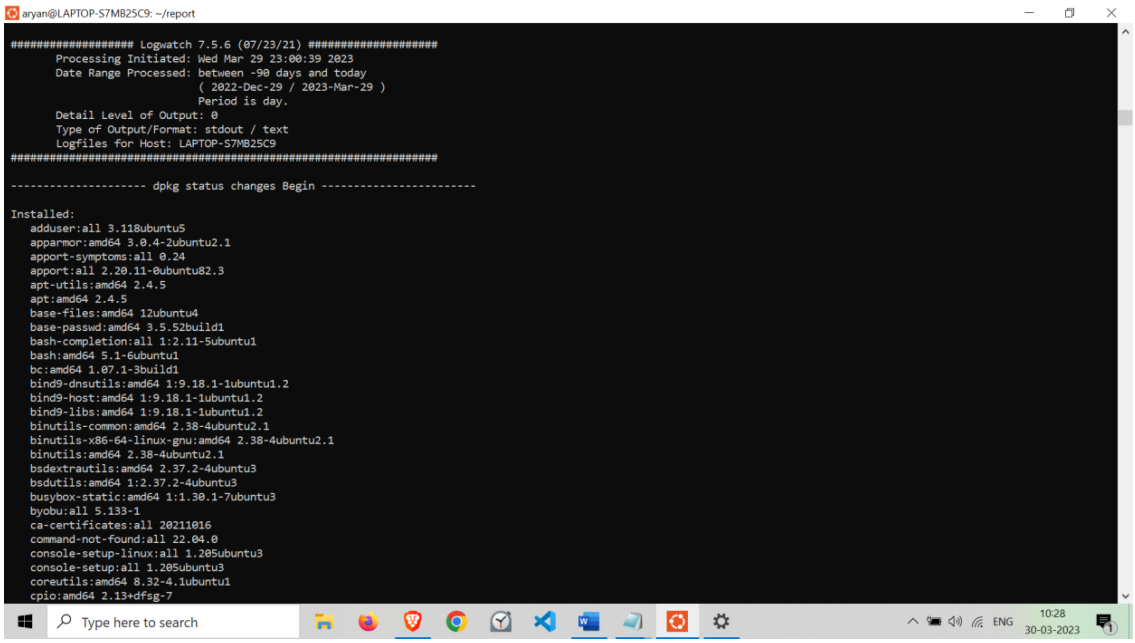
1. 20th March



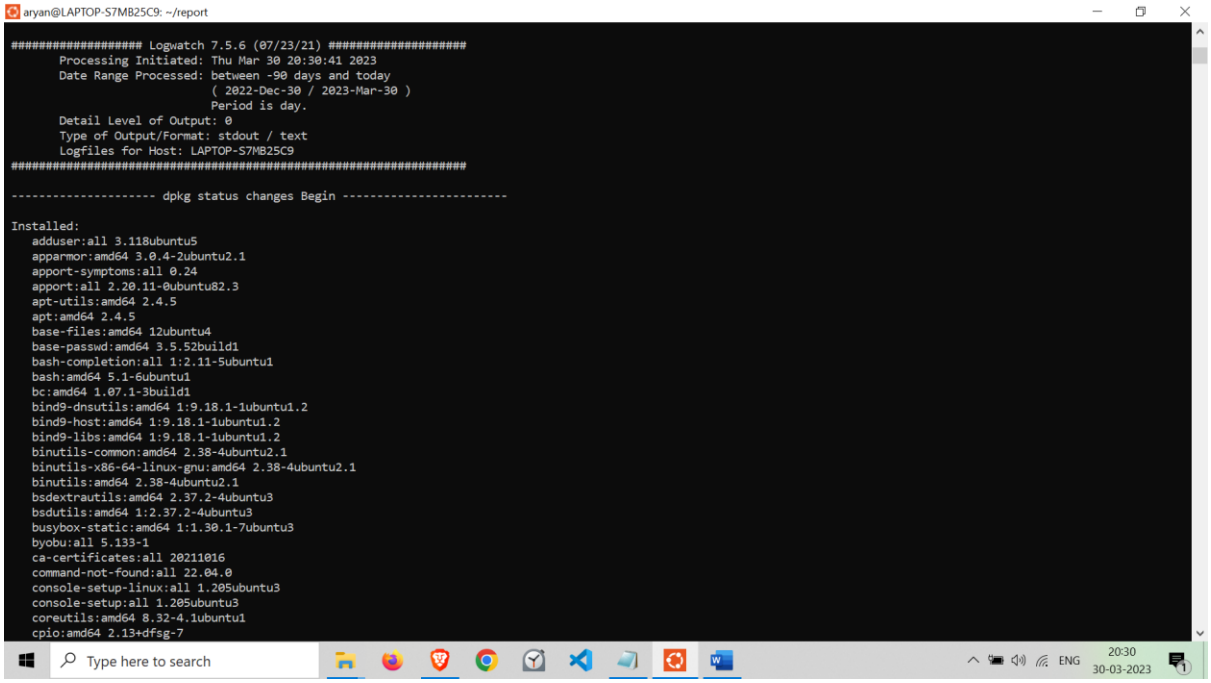
2. 28th March



3. 29th March



4. 30th March



4. Reference

https://ubuntu.com/server/docs/logwatch

https://wiki.archlinux.org/title/Logwatch