**Project Report**

**INT301: OPEN-SOURCE TECHNOLOGY**

Submitted in partial fulfilment of the requirements for the award of degree of

**Batchelor of Technology**

(Computer Science and Engineering)

Submitted to Prof: Dr. Manjot Kaur (28925)

LOVELY PROFESSIONAL UNIVERSITY PHAGWARA, PUNJAB



Submitted By:

Name of student: SPARSH KHANNA

Registration Number: 11914821

GitHub Project Link:

Annexure- IX (b): Student Declaration

**To whom so it may concern**

I, **SPARSH KHANNA,** Registration number: **11914821**, hereby declare that the work done by me on Use **any open-source software to generate a detailed report of your system to investigate what**

**happened on a computer in last 3 months.,** in the month of March 2023, under the supervision of Prof. Dr. Manjot Kaur (28925)School of Computer Science and Engineering at **Lovely Professional University**, Phagwara, Punjab, is a record of original work from the partial fulfilment of the requirements for the award of the degree, **Batchelor of Technology (Computer Science and Engineering).**

Name of the Student: SPARSH KHANNA

Registration Number: 11914821

Dated: 20th Mar 2023

CHAPTER – 1

INTRODUCTION:

1.1 OBJECTIVE OF THE PROJECT:

The objective of this project is to use any open-source software to generate a detailed report of system to investigate what happened on a computer in last 3 months and storing the 3 months log file as a text file. This project aims to provides a simple and effective way to monitor and report system activity on Ubuntu Linux, and can be customized to meet a wide range of system monitoring and investigation needs.

1.2 DESCRIPTION OF THE PROJECT:

This project involves using open-source software to extract activities happened on the computer and extracting it to a pain text. The data which is being extracted is for last 3 months.

The project can be useful for a variety of purposes, forensics analysis. Investigators can view the records that capture the information about the activities and events that occur on a system or device. This information can include login attempts, file access, network activity, and more. By reviewing these logs files, forensic analysts can gain insights into what happened on the system, when its happened and who was involved.

This project can be implemented using various open-source software tools such as “Logwatch” or other similar software. The steps for extracting the data may vary depending on the software used.

Overall, this project provides a simple and effective way to monitor and report system activity on Ubuntu Linux, and can be customized to meet a wide range of system monitoring and investigation needs.

1.3 SCOPE OF THE PROJECT:

The scope of a project defines the boundaries and objectives of the project, including what will be included and what will not. It outlines the deliverables, timeline, budget, and resources required to complete the project successfully. A well-defined project scope helps ensure that everyone involved in the project has a clear understanding of what needs to be accomplished, what resources are required, and what success looks like. It also helps to minimize the risk of scope creep, which occurs when the project's objectives expand beyond the initial scope.

The scope of a project typically includes the following elements:

1. Project Objective: This specifies goal and the outcomes that the project is intended to achieve. This project aims to provides a simple and effective way to monitor and report system activity on Ubuntu Linux, and can be customized to meet a wide range of system monitoring and investigation needs.
2. Deliverables: This specifies the tangible product, services or results that will be produced as a result of the project. This Project Provides us the output file that is System\_activity\_report.txt as and outcome of the project
3. Timeline: In this project Timeline used was 3 months earlier from today’s date

1.4 FLOW CHAT OF THE PROJECT:

**Step1:** Install Linux Ubuntu from Microsoft Store: as referred in figure 1.4.1

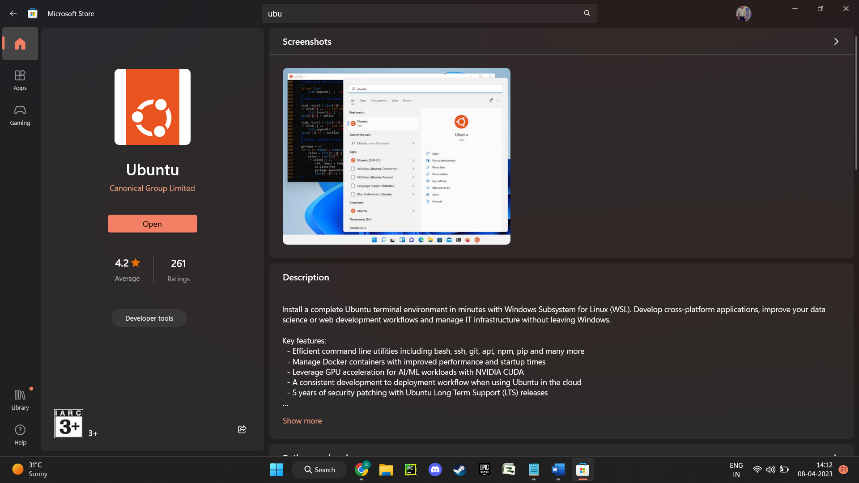


Figure 1.4.1 – Installation of Linux Operating System (UBUNTU)

**Step2:** Install Logwatch on your Ubuntu Linux system

sudo apt-get update

sudo apt-get install logwatch: as referred in Figure 1.4.2

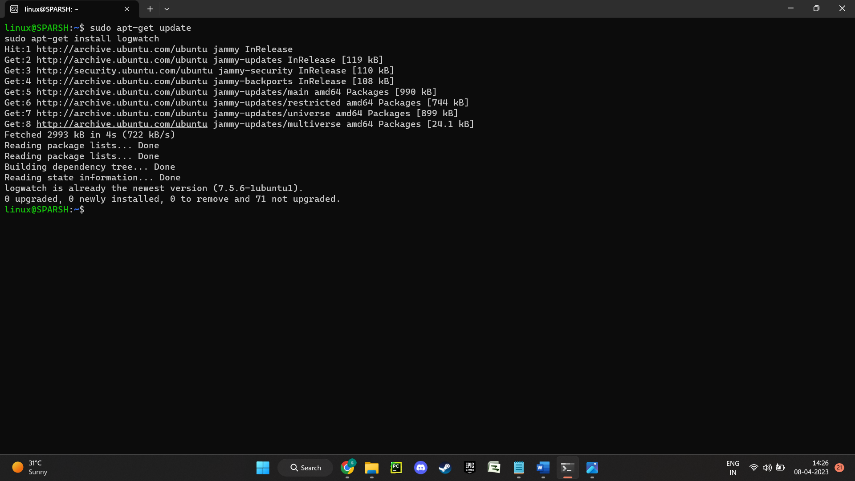


Figure 1.4.2 – Installation of Logwatch tool on Ubuntu Linux Terminal

**Step3:** To generate a detailed report of system activity in the last three months, including information on logins, file modifications, system errors, and other system events.

sudo logwatch --detail 10 --range 'between -90 days and today’: as referred in Figure 1.4.3

# The **--detail** option specifies the level of detail in the report, and the 10 argument specifies the highest level of detail. The **--range** option specifies the time range for the report, and the between **-90 days and today** argument specifies that we want to monitor system activity for the last three months.: as referred in Figure 1.4.4. End of the log details: as referred in figure 1.4.5

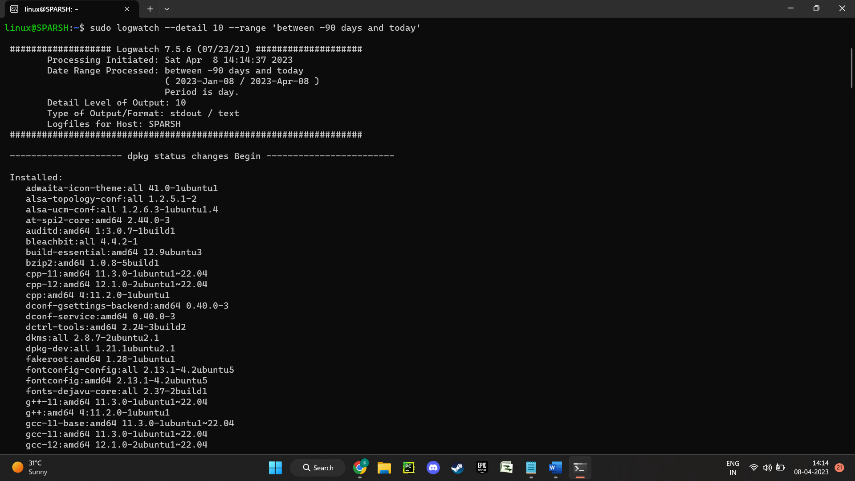


Figure 1.4.3 – Entered code to open the logs for last 3 Months

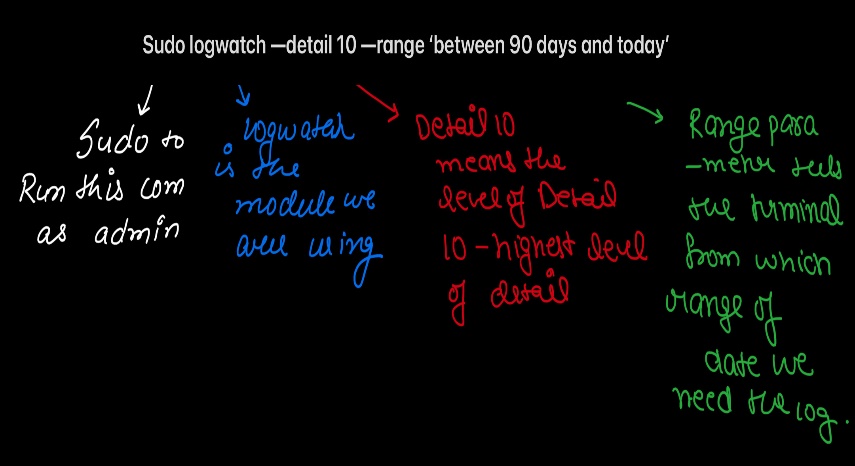


Figure 1.4.4 – Explanation of Code

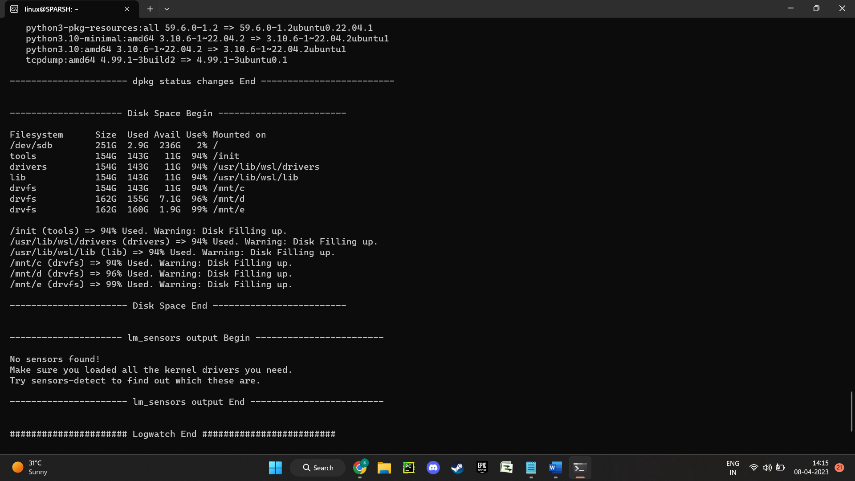


Figure 1.4.5 – End of the logwatch Process

**Step4:** Save the report to a text file named "system\_activity\_report.txt".

sudo logwatch --detail 10 --range 'between -90 days and today' > system\_activity\_report.txt

:as referred in Figure 1.4.5 & Figure 1.4.6

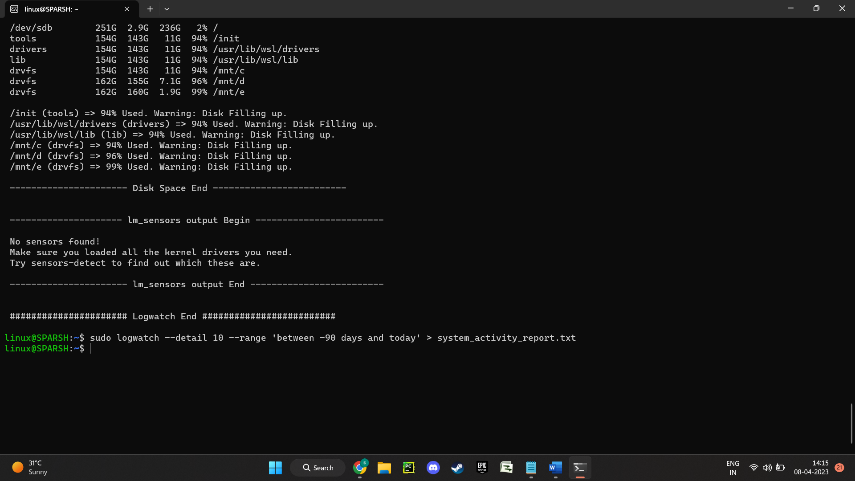


Figure 1.4.5 – Saving the complete log in System\_activity\_report.txt

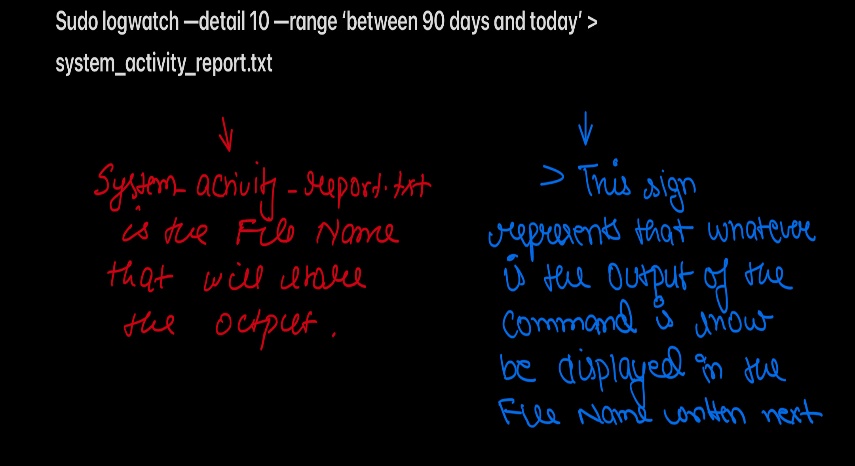


Figure 1.4.6 – Explanation of Code

**Step5:** At [\\wsl.localhost\Ubuntu\home\linux](file:///\\wsl.localhost\Ubuntu\home\linux) You’ll find a file named System\_activity\_report.txt: as referred in Figure 1.4.7

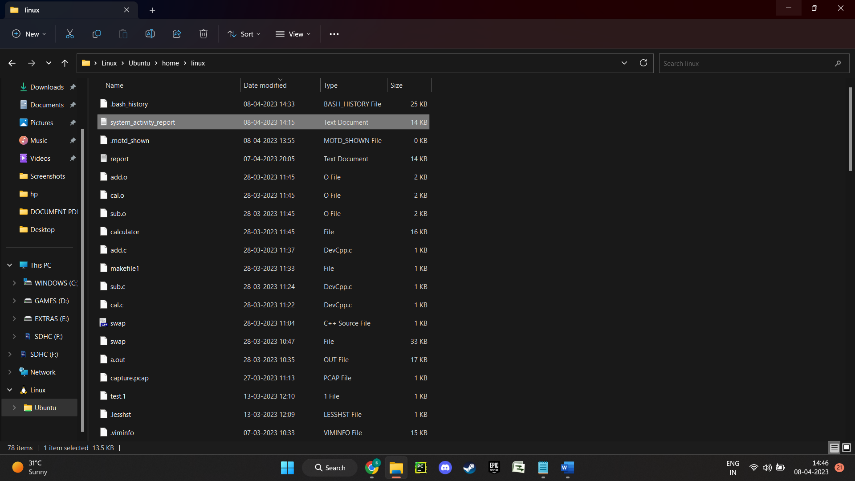


Figure 1.4.7 – System\_activity\_report.txt

CHAPTER – 2

2.1 SYSTEM CONFIGRATIONS

Operating System Used for the project: Linux Ubuntu -v2204.1.8.0

Software Used for the project – Logwatch: as referred in Figure 2.1.1

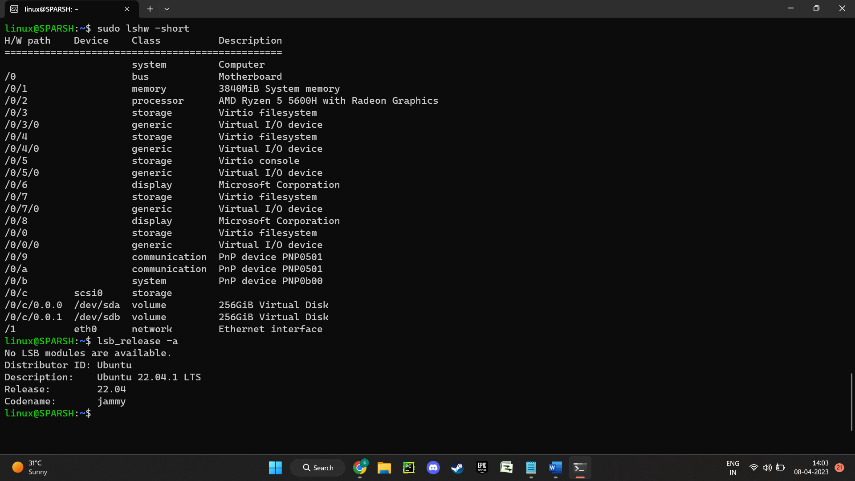


Figure 2.1.1 – System Description

Linux Ubuntu is a popular open-source operating system based on the Linux kernel. It is designed to be user-friendly and easy to use, making it a popular choice for both personal and professional use. Ubuntu's architecture is based on the Debian Linux distribution and uses the GNOME desktop environment. It also includes a wide range of software applications, including web browsers, office productivity suites, media players, and development tools.

The Linux kernel at the core of Ubuntu provides robust security, stability, and performance. Ubuntu also includes features such as automatic software updates and a package management system that allows users to easily install, update, and remove software. One of the key features of Ubuntu is its strong community support. Users can access online forums and documentation to find solutions to common issues and get help from other users. Additionally, Ubuntu's open-source nature allows users to modify and customize the operating systemto their specific needs.

Ubuntu can be installed on a wide range of hardware, from personal computers to servers and even mobile devices. Its versatility and ease of use make it a popular choice for individuals and organizations alike**.**

2.2 REFERENCES

[2.2.1] <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps>

[2.2.2] <https://ubuntu.com/server/docs/logwatch>

[2.2.3] <https://www.tutorialspoint.com/unix_commands/logwatch.htm>

[2.2.4] <https://logit.io/blog/post/open-source-logging-tools/>

[2.2.5] <https://signoz.io/blog/open-source-log-management/>