



LOVELY
PROFESSIONAL
UNIVERSITY

INT 301

CA-3

OPEN-SOURCE TECHNOLOGIES

**Generate your Entire system's log report of past 3 months
along with this find partial and full multimedia Files(video
files) in DataStream**

Name: Simran Mujral

Reg No: 11904577

Section:KE008

School: Computer Science and Engineering

Faculty: Dr. Rajeshwar Sharma

Git Link :

INTRODUCTION

1.1 OBJECTIVE OF THE PROJECT:

The objective of this project is to perform a comprehensive analysis of a system's log files for the past three months using log watch and file light tools. The log watch tool is used to parse the system logs and create a summary report that can provide valuable insights into system performance, security, and other critical metrics. Firelight, on the other hand, is a graphical disk usage analyzer that can be used to visualize the system's file storage structure, identify large files, and pinpoint directories that consume the most disk space.

By combining the information generated by log watch and file light, this project aims to provide a holistic view of the system's performance, identify potential issues that may have occurred in the past three months, and recommend necessary actions to optimize the system's performance and enhance its security.

Moreover, locating partial and full multimedia files such as video files in the DataStream can help identify any files that are consuming a significant amount of disk space, detect any unauthorized or illegal multimedia content, and assess the impact of multimedia content on system performance.

In summary, the objective of this project is to generate a comprehensive log report of a system's past three months of activity and analyze the system's storage structure to locate multimedia files. This will enable system administrators to optimize the system's performance, enhance its security, and ensure that the system is being used appropriately.

1.2 DESCRIPTION OF THE PROJECT :

This project involves using log watch and file light tools to generate a comprehensive log report for a system's activity in the past three months and locate multimedia files, specifically video files, in the system's DataStream. The project can be broken down into the following steps:

- **Install log watch and file light:** The first step is to install log watch and file light tools on the system. These tools can be installed using the system's package manager or by downloading and installing them manually.
- **Configure log watch:** Once log watch is installed, it needs to be configured to generate a summary report of the system's activity for the past three months. The log watch configuration file needs to be edited to specify the log files to be monitored, the frequency of reports, and other settings.

- **Generate log report:** After configuring log watch, it can be run to generate a summary report of the system's activity in the past three months.
- The report includes information such as the number of log entries, the number of errors, warnings, and information messages, and other key metrics.
- **Analyze log report:** The log report generated by log watch can be analyzed to identify potential issues that occurred in the past three months, such as security breaches, system errors, or performance issues. This analysis can help system administrators take corrective actions to improve the system's performance and security.
- **Install file light:** Once log watch is configured and the report is generated, file light can be installed to analyze the system's storage structure and locate multimedia files such as video files.
- **Locate multimedia files:** Firelight provides a graphical representation of the system's storage structure, making it easy to locate multimedia files such as video files. The files can be sorted by size, date, or type to identify large files that may be consuming a significant amount of disk space.
- **Analyze multimedia files:** After locating multimedia files, they can be analyzed to determine their impact on system performance and security. Any unauthorized or illegal multimedia content can be removed, and the system's storage structure can be optimized to improve performance.

In summary, this project involves using log watch and file light tools to generate a comprehensive log report of a system's activity in the past three months and locate multimedia files such as video files in the system's DataStream. The project can help system administrators optimize system performance, enhance security, and ensure appropriate use of the system.

About Log watch :

Log watch is an open-source log parsing and analysis tool that helps system administrators monitor system logs and generate reports on system activity. The tool is designed to simplify log analysis by providing a summary of key metrics and identifying potential issues in the system. Because it makes the process of analyzing log data easier, Log watch is a useful tool for keeping an eye on system logs. A lot of data concerning system activity is contained in system logs, including failures, warnings, and other events. But sorting through this data can be a difficult and time-consuming operation. Through the creation of a summary report of system activity, Log watch streamlines the process of analyzing system logs. The programmer organizes and filters log data to produce a streamlined report that is simpler to read and comprehend. System administrators can monitor system performance, discover potential security threats, and diagnose problems with their systems by using the report that Log watch produces.

About File Light:

Firelight is an open-source graphical disk usage analyzer tool that helps system administrators visualize the distribution of files and directories on a file system. The tool provides a visual representation of the file system structure, making it easy to identify large files and directories that may be consuming a significant amount of disk space.

1.3 SCOPE OF THE PROJECT:

The scope of the project is to generate a comprehensive log report of the system's activity for the past three months using log watch and file light.

- Generate a log report of the system's activity for the past three months using log watch and file light.
- Use log watch to monitor and parse log files generated by various applications such as web servers, mail servers, and other services.
- Configure log watch to analyze logs in real-time or in batches, depending on the system's requirements.
- Customize log watch to monitor the log files and filters specific to the system's requirements.
- Use file light to visualize the distribution of files and directories on the file system, identifying large files and directories that may be consuming a significant amount of disk space.
- Configure file light to identify partial and full multimedia files (video files) in DataStream.
- Use file light to sort files by size, type, or date to identify large files that may be consuming a significant amount of disk space.
- Provide a list of the largest files identified by file light, making it easy to identify and delete files that are no longer needed.
- Generate a report that summarizes the system's activity and key metrics identified by log watch and file light.

- Include any potential security issues identified by log watch in the report, such as failed login attempts or suspicious network activity.

- Present the report to the system administrators for analysis and optimization of system performance, enhancement of security, and compliance with data retention policies and regulatory requirements.

SYSTEM DESCRIPTION

1.1 TARGET SYSTEM DESCRIPTION:

The target system for this project is a computer or server that runs on a Linux operating system. The system should have enough storage space to store log files generated over the past three months and multimedia files that are being analyzed using file light. Additionally, the system should have the following characteristics:

- The system should have log watch and file light installed, configured and running.
- The system should have a centralized logging system that collects and stores logs generated by various applications and services.
- The system should have a web server, mail server, database server or other applications that generate logs that can be monitored by log watch.
- The system should have a DataStream directory that contains multimedia files such as video files.
- The system should have enough processing power to run log watch and file light without affecting the system's performance.
- The system should have adequate network bandwidth to transfer large log files generated by log watch and multimedia files analyzed by file light.
- The system should have appropriate permissions and access controls set up to ensure that only authorized users can access and analyze the log files and multimedia files.
- The system should have a comprehensive backup and recovery system in place to ensure the integrity of the log files and multimedia files.

In summary, the target system for this project is a Linux-based system with log watch and file light installed and configured, a centralized logging system, multimedia files in DataStream directory, and sufficient resources to run log watch and file light without affecting the system's performance. The system should have appropriate access controls and backup and recovery systems in place to ensure the integrity of the log files and multimedia files.

ANALYSIS REPORT

Use Log Watch Open-Source software to generate your entire system's log report of past 3 months

Step 1:

Install Rpm

RPM is used to manage the installation, update, and removal of software packages on a Linux system. Each package is stored in an RPM file that contains the software's binaries, configuration files, and installation scripts.

```
root@MyUbuntuDipraj:~# apt install rpm
Reading package lists... Done
Building dependency tree
Reading state information... Done
You might want to run 'apt --fix-broken install' to correct these.
The following packages have unmet dependencies:
 logwatch : Depends: default-ntp or
               mail-transport-agent
 rpm : Depends: librpm8 (>= 4.14.2+dfsg1) but it is not going to be installed
       Depends: librpmbuild8 (>= 4.14.0+dfsg1) but it is not going to be installed
       Depends: librpmio8 (>= 4.14.0+dfsg1) but it is not going to be installed
       Depends: librpmnsign8 (>= 4.14.0+dfsg1) but it is not going to be installed
       Depends: rpmscript but it is not going to be installed
       Depends: debugedit (= 4.14.2.1+dfsg1-1build2) but it is not going to be installed
       Depends: rpm-common (= 4.14.2.1+dfsg1-1build2) but it is not going to be installed
E: Unmet dependencies. Try 'apt --fix-broken install' with no packages (or specify a solution).
root@MyUbuntuDipraj:~# apt --fix-broken
Command line option --fix-broken is not understood in combination with the other options
root@MyUbuntuDipraj:~# apt --fix-broken install
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
```

Step 2:

First go to the */etc/cron.daily* folder and open *00logwatch* file ,

If root mail was set no need to change other wise, need to change the root mail option to user mail.

```
root@MyUbuntuDipraj:~# cd /etc/cron.daily/
root@MyUbuntuDipraj:/etc/cron.daily# ls
00logwatch 0anacron apport apt-compat bsdmainutils cracklib-runtime dpkg google-chrome logrotate nan-db popularity-contest update-notifi
root@MyUbuntuDipraj:/etc/cron.daily# nano 00logwatch
```

Otherwise type 'mail' command and check there any mail set for the Root user.

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@MyUbuntuDipraj:/etc/cron.daily# mail
to mail for root
root@MyUbuntuDipraj:/etc/cron.daily# cd
```

Step 3:

If there was no logwatch.conf file in the */etc/logwatch/conf/* folder then install Logwatch.

```
root@MyUbuntuDipraj:~# cd /etc/logwatch/
root@MyUbuntuDipraj:/etc/logwatch# ls
conf scripts
root@MyUbuntuDipraj:/etc/logwatch# cd conf/
root@MyUbuntuDipraj:/etc/logwatch/conf# ls
profiles services
root@MyUbuntuDipraj:/etc/logwatch/conf# cd services/
root@MyUbuntuDipraj:/etc/logwatch/conf/services# ls
```

Install Log watch

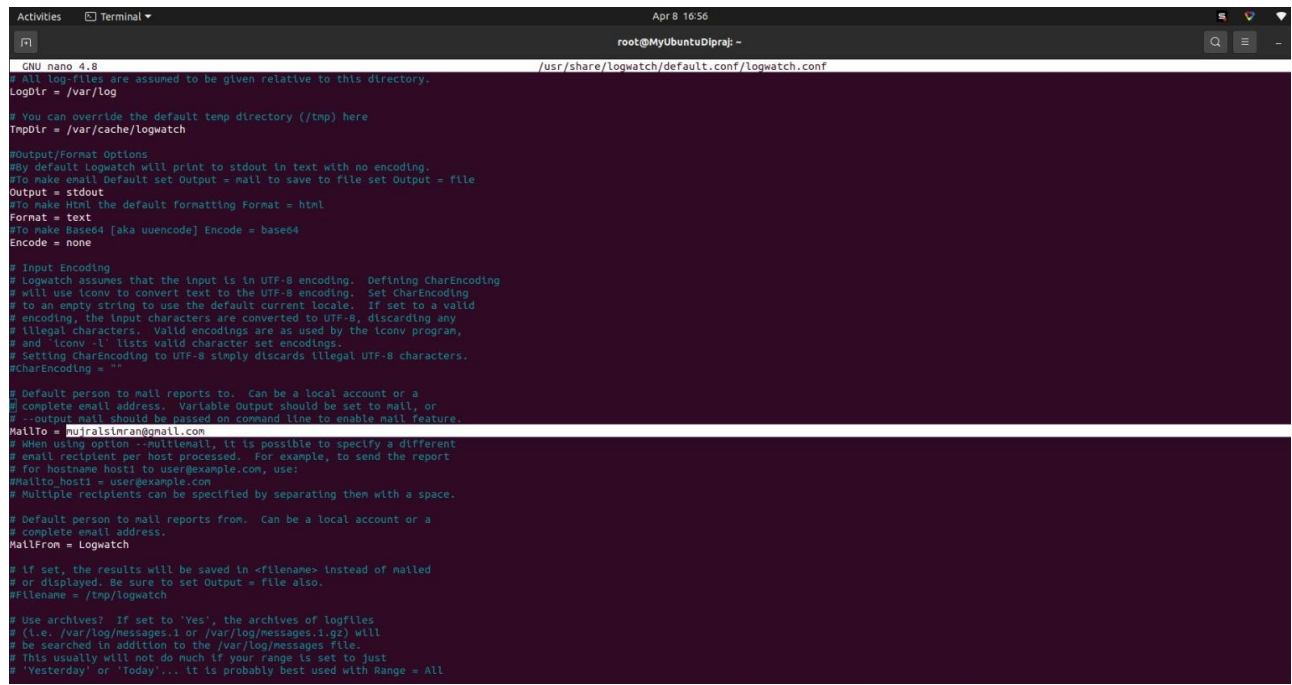
```
root@MyUbuntuDipraj:~# apt-get install logwatch
Reading package lists... Done
Building dependency tree
Reading state information... Done
logwatch is already the newest version (7.5.2-1ubuntu1.3).
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra glib2.0-gstreamer1.0 vaapi libfwupdplugin1 libgstreamer-plugins-bad1.0-0 libnvidia-cfgi-510 libnvidia-common-510 libnvidia-decode-510 libnvidia-encode-510
  libnvidia-extra-510 libnvidia-fbc1-510 libnvidia-gl-510 libxi1-xcb1:amd64 libxmb1 nvidia-compute-utils-510 nvidia-kernel-source-510 nvidia-settings nvidia-utils-510 screen-resolution-extra
  xserver-xorg-video-nvidia-510
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
root@MyUbuntuDipraj:~# nano /usr/share/logwatch/default.conf/logwatch.conf
root@MyUbuntuDipraj:~# sudo logwatch --service all --detail high --mailto diprajdaripabnk@gmail.com --range yesterday
You have new mail in /var/mail/root
```

Step 4:

if Mail was not set for the root user, then open file /usr/share/logwatch/default.conf/logwatch.conf/ and set the mail in Mailto parameter.

```
root@MyUbuntuDipraj:~# nano /usr/share/logwatch/default.conf/logwatch.conf
```

If Not set then set the Mailto parameter



```
Activities Terminal Apr 8 16:56
root@MyUbuntuDipraj:~
GNU nano 4.8 /usr/share/logwatch/default.conf/logwatch.conf
# All log-files are assumed to be given relative to this directory.
LogDir = /var/log

# You can override the default temp directory (/tmp) here
TmpDir = /var/cache/logwatch

#Output/Format Options
#By default Logwatch will print to stdout in text with no encoding.
#To make email Default set Output = mail to save to file set Output = file
Output = stdout
#To make html the default formatting Format = html
Format = text
#To make Base64 [aka uuencode] Encode = base64
Encode = none

# Input Encoding
# Logwatch assumes that the input is in UTF-8 encoding. Defining CharEncoding
# will use iconv to convert text to the UTF-8 encoding. Set CharEncoding
# to an empty string to use the default current locale. If set to a valid
# encoding, the input characters are converted to UTF-8, discarding any
# illegal characters. Valid encodings are as used by the iconv program,
# and 'iconv -l' lists valid character set encodings.
# Setting CharEncoding to UTF-8 simply discards illegal UTF-8 characters.
CharEncoding = ""

# Default person to mail reports to. Can be a local account or a
# complete email address. Variable Output should be set to mail, or
# --output mail should be passed on command line to enable mail feature.
MailTo = hujralsinrang@gmail.com
# When using option --multimail, it is possible to specify a different
# email recipient per host processed. For example, to send the report
# for hostname host1 to user@example.com, use:
#Mailto_host1 = user@example.com
# Multiple recipients can be specified by separating them with a space.

# Default person to mail reports from. Can be a local account or a
# complete email address.
MailFrom = Logwatch

# If set, the results will be saved in <filename> instead of mailed
# or displayed. Be sure to set Output = file also.
Filename = /tmp/logwatch

# Use archives? If set to 'Yes', the archives of logfiles
# (i.e. /var/log/messages.1 or /var/log/messages.1.gz) will
# be searched in addition to the /var/log/messages file.
# This usually will not do much if your range is set to just
# 'Yesterday' or 'Today'... It is probably best used with Range = All
```

Step 5:

For Check 3 Months / 90 days log run this command.

And redirect the output of last 3 months log in log_report.txt file.

Sudo log watch --range 'between -90 days and today'.

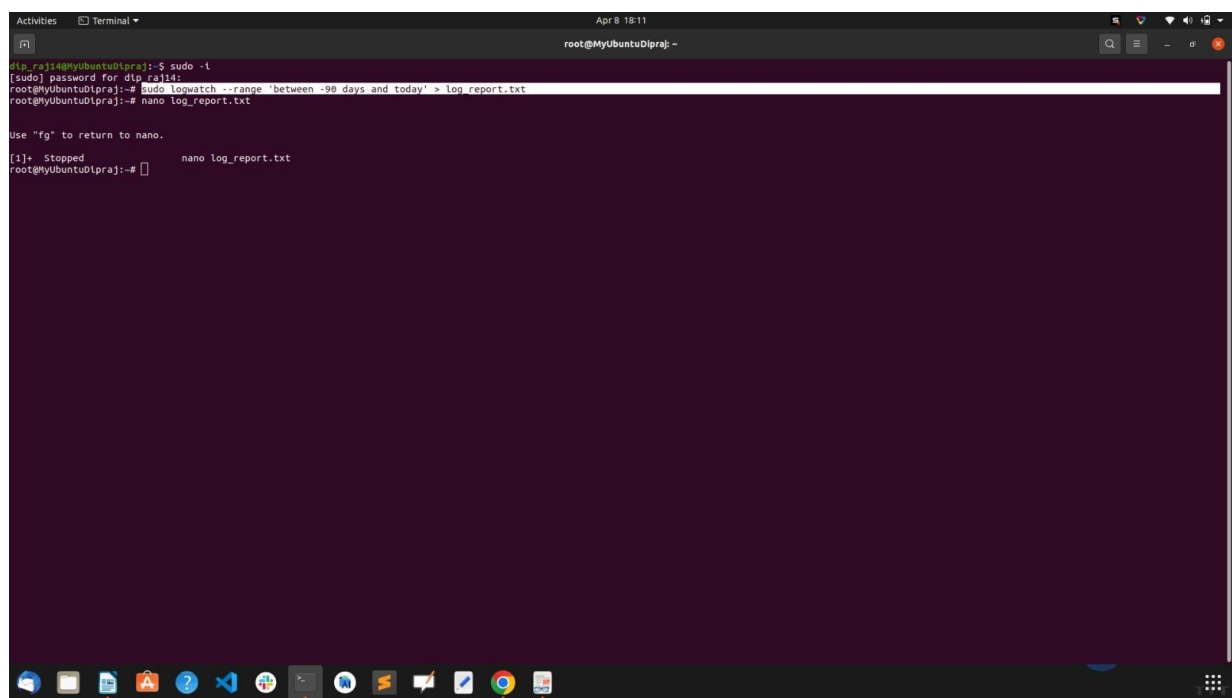
The command "sudo logwatch --range 'between -90 days and today'" is used to generate a log report for the system over the past 90 days. Here's a breakdown of the command and its components:

- "sudo" is a command used in Linux to run a command with elevated privileges or as a different user. It allows the user to execute a command as the root user, which has unrestricted access to the system.
- "log watch" is a command-line tool that analyzes log files and generates a report that summarizes the system's activities and events.

"--range" is an option used to specify a date range for the log report. The date range is specified using the format "between start-date and end-date".

- "'between -90 days and today'" is the date range specified for this command. It tells logwatch to generate a report for events that occurred between 90 days ago and today.
- The "-" sign before "90" indicates that the date range is relative to the current date, and "today" indicates that the report should include events up to the current time.

So, the command "sudo log watch --range 'between -90 days and today'" generates a log report that summarizes the system's activities and events for the past 90 days, starting from 90 days ago and up to the current time. It provides an overview of the system's log data, making it easier to monitor and troubleshoot any issues that may have occurred during this time.



```
Activities Terminal Apr 8 18:11
root@MyUbuntuDlpraj: ~
dtp_raj14@MyUbuntuDlpraj:~$ sudo -l
[sudo] password for dtp_raj14:
root@MyUbuntuDlpraj:~$ sudo logwatch --range 'between -90 days and today' > log_report.txt
root@MyUbuntuDlpraj:~$ nano log_report.txt

Use "fg" to return to nano.
[1]+  Stopped                  nano log_report.txt
root@MyUbuntuDlpraj:~$
```


To watch the report run this nano **log_report.txt**.

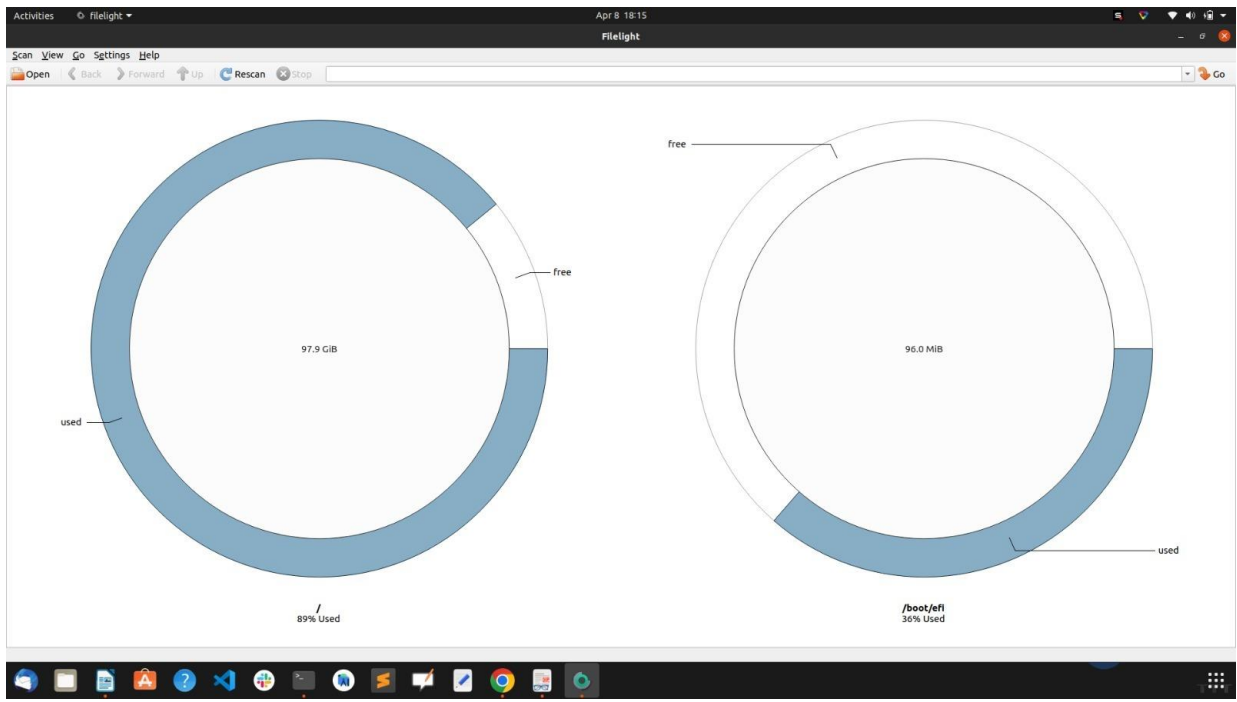
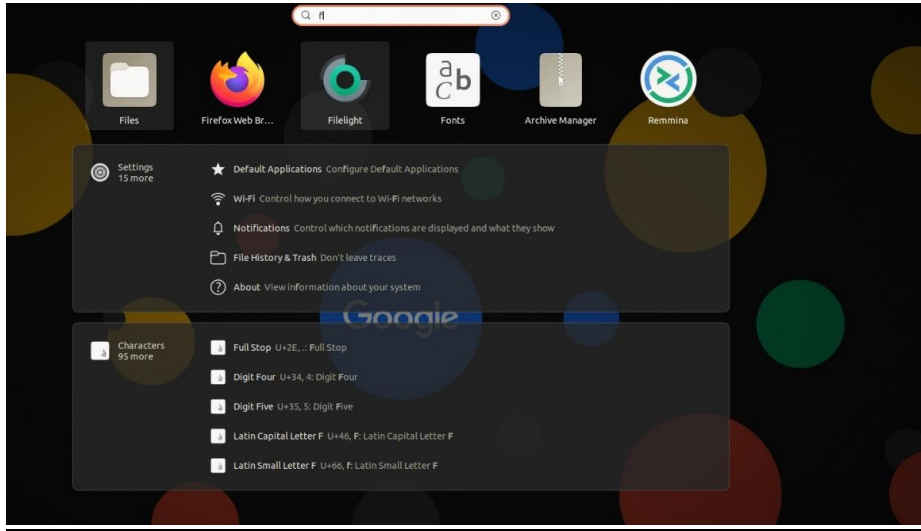
To watch the report run this nano **log_report.txt**.

Step 1:

[illegible]

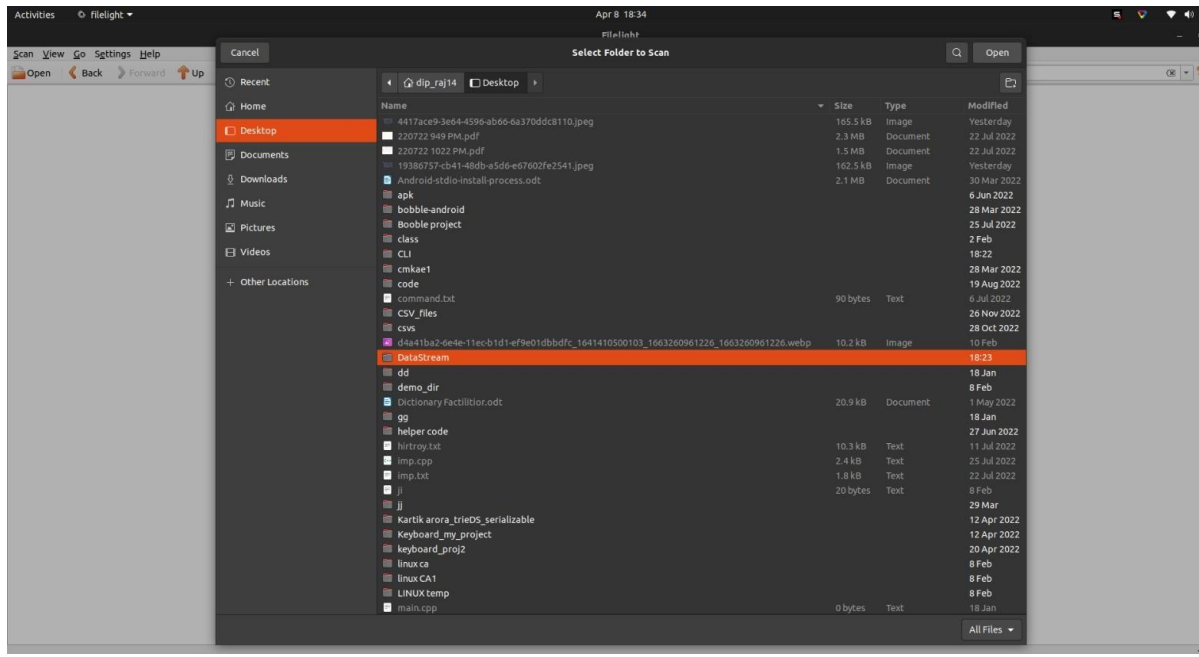
Step 2:

Launch Firelight: Once you have installed Firelight, launch it from your application menu.



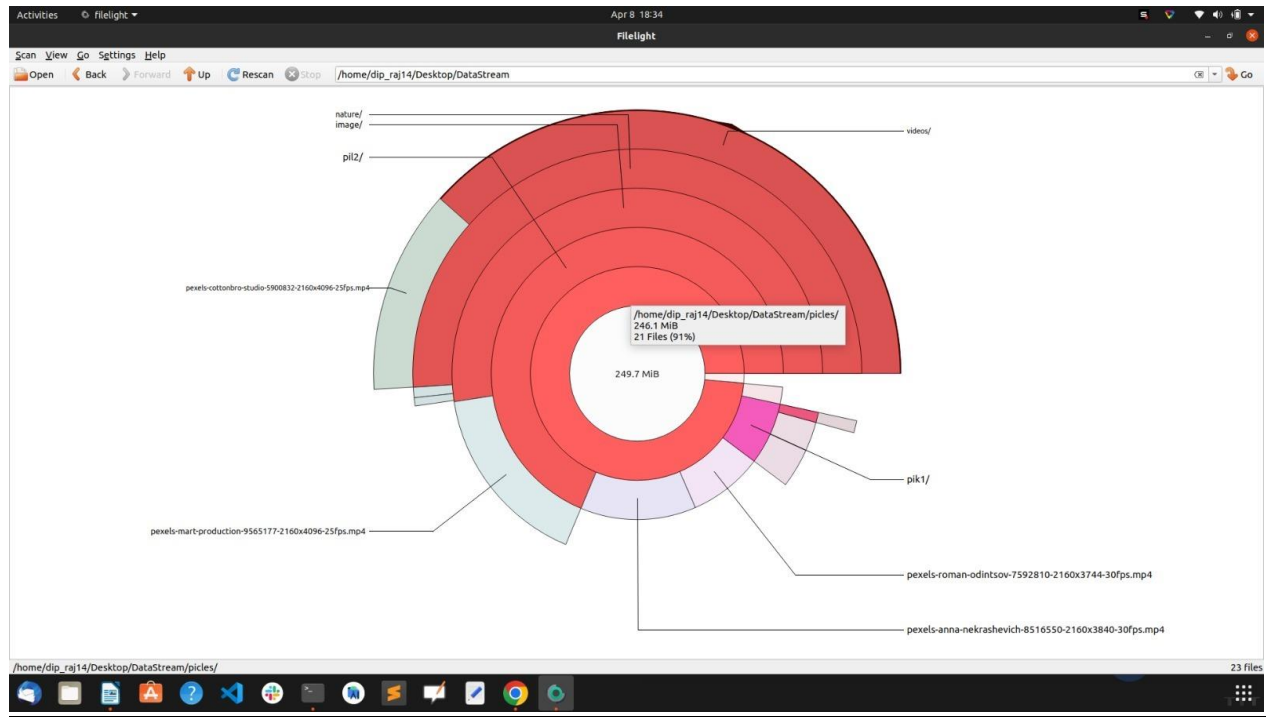
Step 3:

Choose the DataStream folder: In Filelight's main window, navigate to the folder that contains your DataStream. You can do this by clicking on the folders and subfolders in the visual representation of your file system.

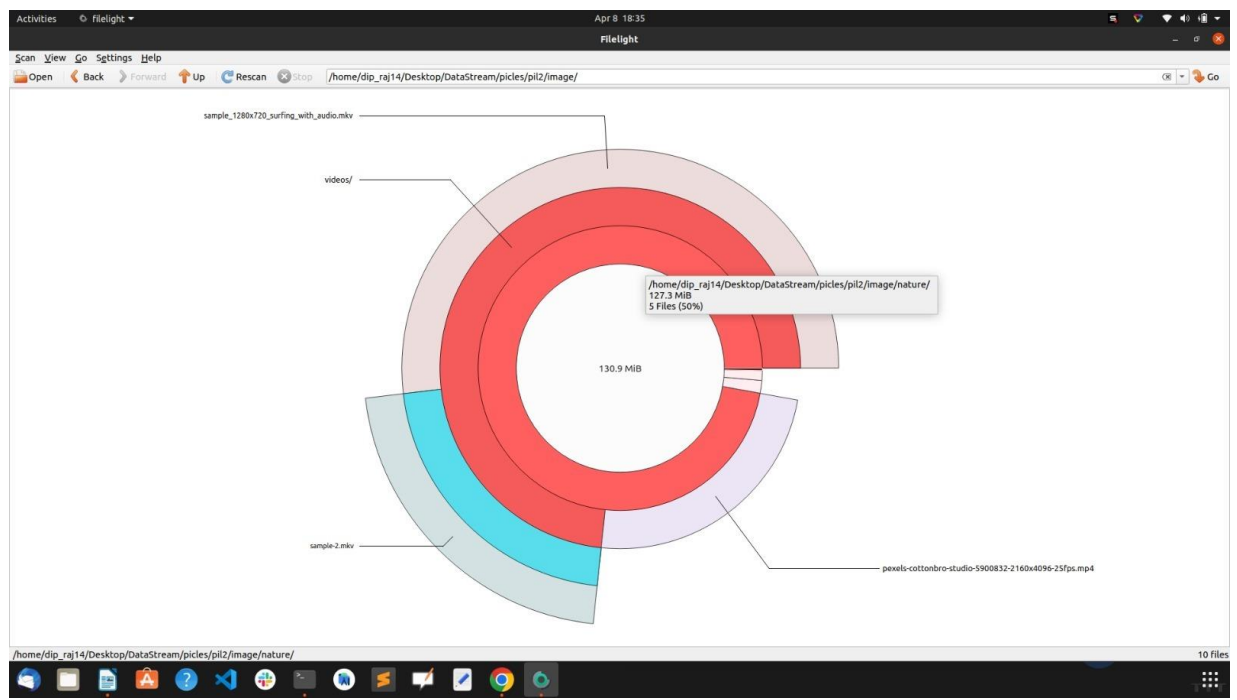


Analyze the folder: Once you have selected the DataStream folder, Firelight will start analyzing its contents. This may take some time, depending on the size of the folder.

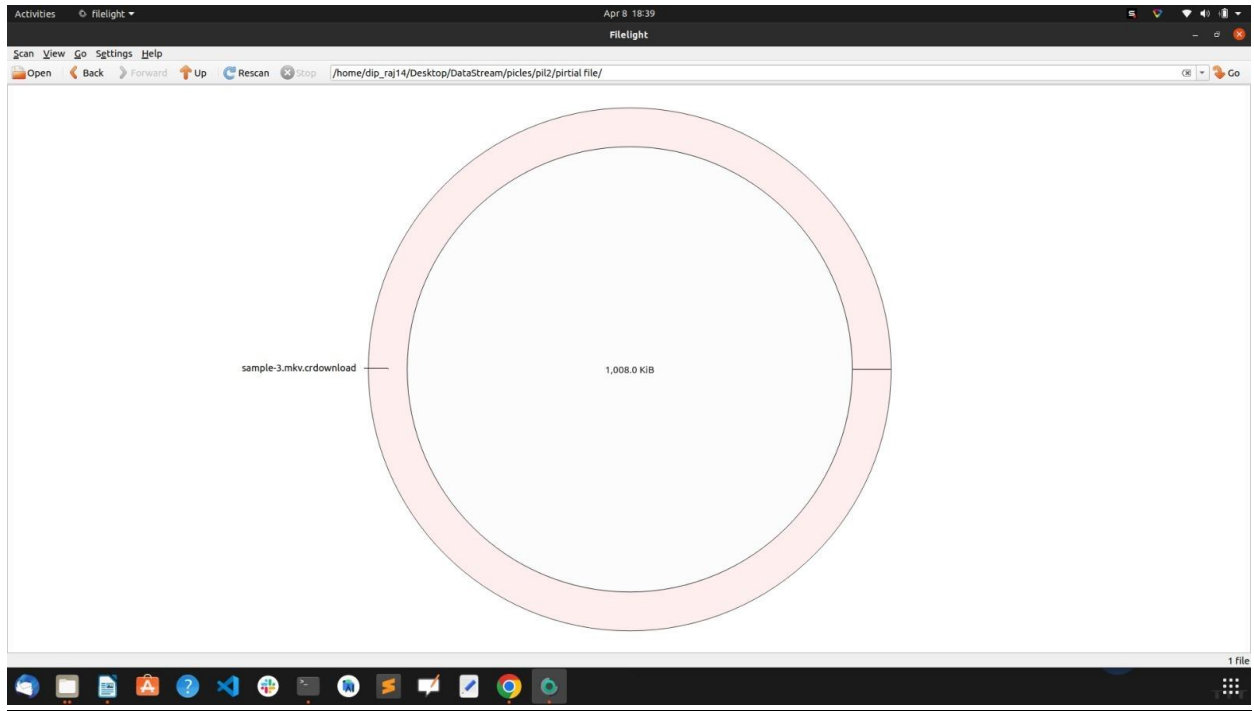
Find video files: Once the analysis is complete, you will see a visual representation of the DataStream folder in Firelight's main window. Look for areas of the visualization that are colored differently from the rest. These represent folders or files that are taking up a lot of storage space.



Identify multimedia files: Look for files with video file extensions such as .mp4, .avi, .mkv, or .mov. These are likely to be multimedia files such as videos.



Identify partial files: If you see a file with an unusual extension or an incomplete name, it may be a partial file. These are files that have not finished downloading or copying and may be incomplete.



Analyze further: If you find a suspicious file, you can right-click on it and select "Properties" to see more information about it, such as its size, creation date, and modification date.

By following these steps, you can use Firelight to find both partial and full multimedia files (video files) in your DataStream folder.

BIBLIOGRAPHY

[google.com](https://www.google.com)

[wikipedia.org](https://www.wikipedia.org)

[LogWatch Doc](#)

[FileLight Download](#)

[GitHub](#)