

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.

Ans: The open-source software I am going to use is logwatch.

**Command: sudo logwatch --range 'between -90 days and today'**

**Command for saving in the file.**

**sudo logwatch --range 'between -90 days and today'>systemreport.txt**

## **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, its 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-based 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.

```

aryan@LAPTOP-S7MB25C9: ~/report
##### Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Wed Mar 29 23:00:39 2023
Date Range Processed: between -90 days and today
                      ( 2022-Dec-29 / 2023-Mar-29 )
                      Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: LAPTOP-S7MB25C9
#####

----- dpkg status changes Begin -----

Installed:
adduser:all 3.118ubuntu5
apparmor:amd64 3.0.4-2ubuntu2.1
appport-symlinks:all 0.24
appport:all 2.20.11-0ubuntu2.3
apt-utils:amd64 2.4.5
apt:amd64 2.4.5
base-files:amd64 12ubuntu4
base-passwd:amd64 3.5.52build1
bash-completion:all 1:2.11-5ubuntu1
bash:amd64 5.1-6ubuntu1
bc:amd64 1.07.1-3build1
bind9-dnsutils:amd64 1:9.18.1-1ubuntu1.2
bind9-host:amd64 1:9.18.1-1ubuntu1.2
bind9-libs:amd64 1:9.18.1-1ubuntu1.2
binutils-common:amd64 2.38-4ubuntu2.1
binutils-x86-64-linux-gnu:amd64 2.38-4ubuntu2.1
binutils:amd64 2.38-4ubuntu2.1
bsdextrautils:amd64 2.37.2-4ubuntu3
bsdutils:amd64 1:2.37.2-4ubuntu3
busybox-static:amd64 1:1.30.1-7ubuntu3
byobu:all 5.133-1
ca-certificates:all 20211016
command-not-found:all 22.04.0
console-setup-linux:all 1.205ubuntu3
console-setup:all 1.205ubuntu3
coreutils:amd64 8.32-4.1ubuntu1
cpio:amd64 2.13+dfsg-7

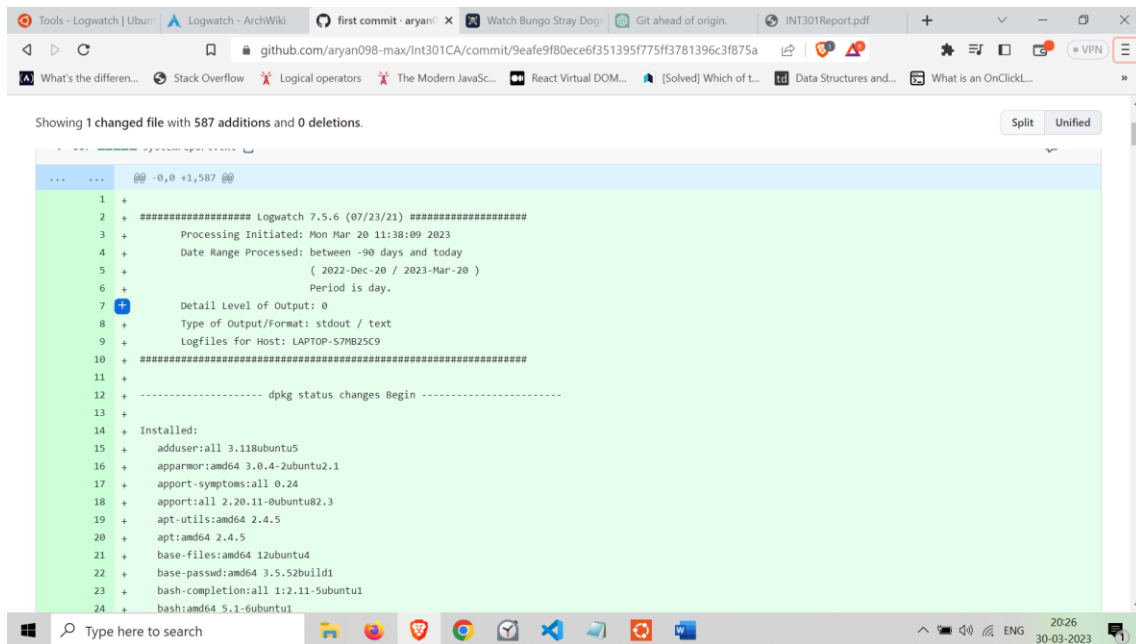
```

### 3. Analysis Report

The analysis report of this project would be summary 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

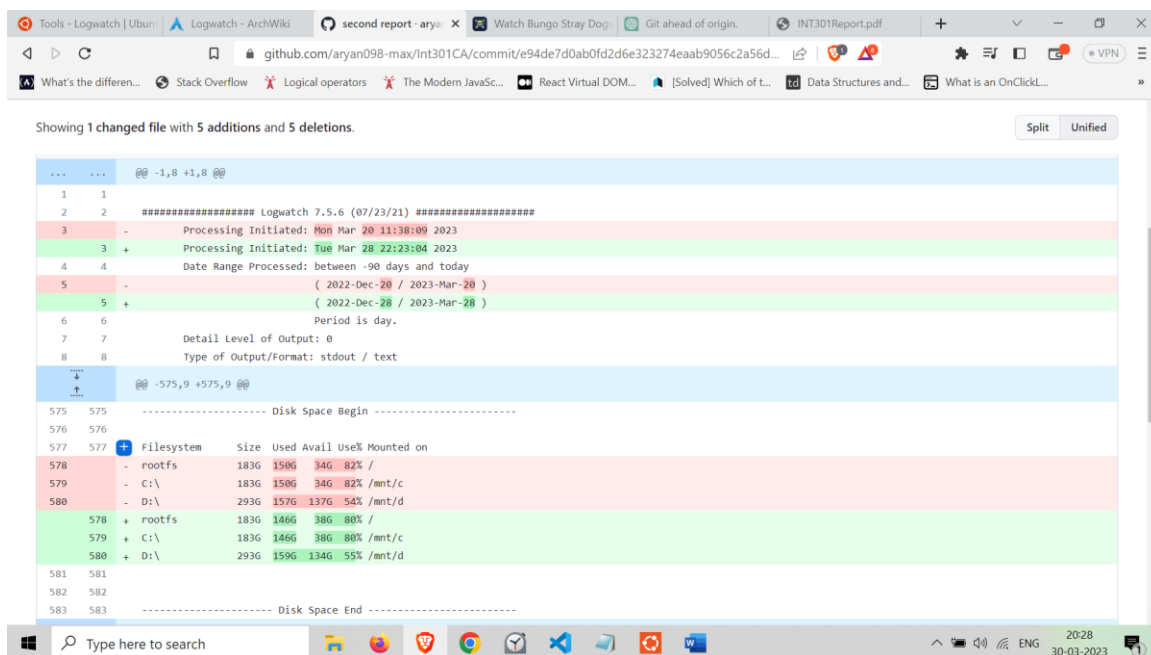
##### 1. 20<sup>th</sup> March



The screenshot shows a GitHub commit diff for the file 'first commit - aryan'. The commit message is 'first commit - aryan'. The diff shows a single file change with 587 additions and 0 deletions. The content of the file is a Logwatch report for March 20, 2023. The report includes details about the system, including the date range processed (2022-Dec-20 to 2023-Mar-20), the period (day), and the detail level of output (0). It also lists the installed packages and their versions.

```
... @@ -0,0 +1,587 @@
1 + ##### Logwatch 7.5.6 (07/23/21) #####
2 + Processing Initiated: Mon Mar 20 11:38:09 2023
3 + Date Range Processed: between -90 days and today
4 + ( 2022-Dec-20 / 2023-Mar-20 )
5 + Period is day.
6 + Detail Level of Output: 0
7 + Type of Output/Format: stdout / text
8 + Logfiles for Host: LAPTOP-57MB25C9
9 + #####
10 + ----- dpkg status changes Begin -----
11 +
12 + Installed:
13 +
14 + adduser:amd64 3.118ubuntu5
15 + apparmor:amd64 3.0.4-2ubuntu2.1
16 + apport-symptoms:amd64 0.24
17 + apport:amd64 2.20.11-0ubuntu2.3
18 + apt-utils:amd64 2.4.5
19 + apt:amd64 2.4.5
20 + base-files:amd64 12ubuntu4
21 + base-passwd:amd64 3.5.52build1
22 + bash-completion:amd64 1:2.11-5ubuntu1
23 + bash:amd64 5.1-5ubuntu1
```

##### 2. 28<sup>th</sup> March



The screenshot shows a GitHub commit diff for the file 'second report - aryan'. The commit message is 'second report - aryan'. The diff shows a single file change with 5 additions and 5 deletions. The content of the file is a Logwatch report for March 28, 2023. The report includes details about the system, including the date range processed (2022-Dec-28 to 2023-Mar-28), the period (day), and the detail level of output (0). It also lists the installed packages and their versions.

```
... @@ -1,8 +1,8 @@
1 1
2 2 ##### Logwatch 7.5.6 (07/23/21) #####
3 - Processing Initiated: Mon Mar 20 11:38:09 2023
3 + Processing Initiated: Tue Mar 28 22:23:04 2023
4 - Date Range Processed: between -90 days and today
4 + Date Range Processed: between -90 days and today
5 - ( 2022-Dec-20 / 2023-Mar-20 )
5 + ( 2022-Dec-28 / 2023-Mar-28 )
6 - Period is day.
6 + Period is day.
7 - Detail Level of Output: 0
7 + Detail Level of Output: 0
8 - Type of Output/Format: stdout / text
8 + Type of Output/Format: stdout / text
... @@ -575,9 +575,9 @@
575 575 ----- Disk Space Begin -----
576 576
577 577 + Filesystem      Size  Used Avail Use% Mounted on
578 - rootfs           1836  1506   346   82% /
579 - C:\              1836  1506   346   82% /mnt/c/
580 - D:\              2936  1576  1376   54% /mnt/d/
578 + rootfs           1836  1466   386   80% /
579 + C:\              1836  1466   386   80% /mnt/c/
580 + D:\              2936  1596  1346   55% /mnt/d/
581 581
582 582 ----- Disk Space End -----
583 583
```

### 3. 29<sup>th</sup> March

```
aryan@LAPTOP-S7MB25C9: ~/report
##### Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Wed Mar 29 23:00:39 2023
Date Range Processed: between -90 days and today
                      ( 2022-Dec-29 / 2023-Mar-29 )
Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: LAPTOP-S7MB25C9
#####
----- dpkg status changes Begin -----

Installed:
adduser:all 3.118ubuntu5
apparmor:amd64 3.0.4-2ubuntu2.1
appport-symptoms:all 0.24
appport:all 2.20.11-0ubuntu82.3
apt-utils:amd64 2.4.5
apt:amd64 2.4.5
base-files:amd64 12ubuntu4
base-passwd:amd64 3.5.52build1
bash-completion:all 1:2.11-5ubuntu1
bash:amd64 5.1-6ubuntu1
bc:amd64 1.07.1-3build1
bind9-dnswriter:amd64 1:9.18.1-1ubuntu1.2
bind9-host:amd64 1:9.18.1-1ubuntu1.2
bind9-libs:amd64 1:9.18.1-1ubuntu1.2
binutils-common:amd64 2.38-4ubuntu2.1
binutils-x86-64-linux-gnu:amd64 2.38-4ubuntu2.1
binutils:amd64 2.38-4ubuntu2.1
bsdextrautils:amd64 2.37.2-4ubuntu3
bsdutils:amd64 1:2.37.2-4ubuntu3
busybox-static:amd64 1:1.30.1-7ubuntu3
byobu:all 5.133-1
ca-certificates:all 20211016
command-not-found:all 22.04.0
console-setup-linux:all 1.205ubuntu3
console-setup:all 1.205ubuntu3
coreutils:amd64 8.32-4.1ubuntu1
cpio:amd64 2.13+dfsg-7
```

### 4. 30<sup>th</sup> March

```
aryan@LAPTOP-S7MB25C9: ~/report
##### Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Thu Mar 30 20:30:41 2023
Date Range Processed: between -90 days and today
                      ( 2022-Dec-30 / 2023-Mar-30 )
Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: LAPTOP-S7MB25C9
#####
----- dpkg status changes Begin -----

Installed:
adduser:all 3.118ubuntu5
apparmor:amd64 3.0.4-2ubuntu2.1
appport-symptoms:all 0.24
appport:all 2.20.11-0ubuntu82.3
apt-utils:amd64 2.4.5
apt:amd64 2.4.5
base-files:amd64 12ubuntu4
base-passwd:amd64 3.5.52build1
bash-completion:all 1:2.11-5ubuntu1
bash:amd64 5.1-6ubuntu1
bc:amd64 1.07.1-3build1
bind9-dnswriter:amd64 1:9.18.1-1ubuntu1.2
bind9-host:amd64 1:9.18.1-1ubuntu1.2
bind9-libs:amd64 1:9.18.1-1ubuntu1.2
binutils-common:amd64 2.38-4ubuntu2.1
binutils-x86-64-linux-gnu:amd64 2.38-4ubuntu2.1
binutils:amd64 2.38-4ubuntu2.1
bsdextrautils:amd64 2.37.2-4ubuntu3
bsdutils:amd64 1:2.37.2-4ubuntu3
busybox-static:amd64 1:1.30.1-7ubuntu3
byobu:all 5.133-1
ca-certificates:all 20211016
command-not-found:all 22.04.0
console-setup-linux:all 1.205ubuntu3
console-setup:all 1.205ubuntu3
coreutils:amd64 8.32-4.1ubuntu1
cpio:amd64 2.13+dfsg-7
```

1<sup>st</sup> April

```
##### Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Sat Apr  1 22:24:21 2023
Date Range Processed: between -90 days and today
                      ( 2023-Jan-01 / 2023-Apr-01 )
                      Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: LAPTOP-S7MB25C9
#####

----- dpkg status changes Begin -----

Installed:
  adduser:all 3.118ubuntu5
  apparmor:amd64 3.0.4-2ubuntu2.1
  apport-symptoms:all 0.24
  apport:all 2.20.11-0ubuntu82.3
  apt-utils:amd64 2.4.5
  apt:amd64 2.4.5
  base-files:amd64 12ubuntu4
  base-passwd:amd64 3.5.52build1
  bash-completion:all 1:2.11-5ubuntu1
  bash:amd64 5.1-6ubuntu1
  bc:amd64 1.07.1-3build1
  bind9-dnsutils:amd64 1:9.18.1-1ubuntu1.2
  bind9-host:amd64 1:9.18.1-1ubuntu1.2
  bind9-libs:amd64 1:9.18.1-1ubuntu1.2
  binutils-common:amd64 2.38-4ubuntu2.1
  binutils-x86-64-linux-gnu:amd64 2.38-4ubuntu2.1
```

```
Removed:
  libdate-manip-perl:all 6.86-1
  logwatch:all 7.5.6-1ubuntu1
  logwatch:all 7.5.6-1ubuntu1
  logwatch:all 7.5.6-1ubuntu1

Purged:
  logwatch:all 7.5.6-1ubuntu1
  logwatch:all 7.5.6-1ubuntu1
  logwatch:all 7.5.6-1ubuntu1

----- dpkg status changes End -----

----- Disk Space Begin -----

Filesystem      Size  Used Avail Use% Mounted on
rootfs          183G  151G   33G  83% /
C:\              183G  151G   33G  83% /mnt/c
D:\              293G  159G  134G  55% /mnt/d

----- Disk Space End -----

##### Logwatch End #####
```

7<sup>th</sup> April

```
aryan@LAPTOP-S7MB25C9: ~/report
aryan@LAPTOP-S7MB25C9:~/report$ sudo logwatch --range 'between -90 days and today'
[sudo] password for aryan:

##### Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Fri Apr 7 20:26:06 2023
Date Range Processed: between -90 days and today
                     ( 2023-Jan-07 / 2023-Apr-07 )
Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: LAPTOP-S7MB25C9
#####

----- dpkg status changes Begin -----

Installed:
bc:amd64 1.07.1-3build1
cpp-11:amd64 11.3.0-1ubuntu1~22.04
cpp:amd64 4:11.2.0-1ubuntu1
fontconfig-config:all 2.13.1-4.2ubuntu5
fonts-dejavu-core:all 2.37-2build1
gcc-11-base:amd64 11.3.0-1ubuntu1~22.04
gcc-11:amd64 11.3.0-1ubuntu1~22.04
gcc:amd64 4:11.2.0-1ubuntu1
gdb:amd64 12.1.0-ubuntu1~22.04
libasan6:amd64 11.3.0-1ubuntu1~22.04
libatomic1:amd64 12.1.0-2ubuntu1~22.04
libbabeltrace1:amd64 1.5.8-2build1
libboost-regex1.74.0:amd64 1.74.0-14ubuntu3
libc-dev-bin:amd64 2.35-0ubuntu3.1
libc-devtools:amd64 2.35-0ubuntu3.1
libc6-dbg:amd64 2.35-0ubuntu3.1
libc6-dev:amd64 2.35-0ubuntu3.1
libc6i-0:amd64 12.1.0-2ubuntu1~22.04
libcrypt-dev:amd64 1:4.4.27-1
libdate-manip-perl:all 6.86-1
libdate-manip-perl:all 6.86-1
libdebuginfod-common:all 0.186-1build1
libdebuginfod1:amd64 0.186-1build1
libdeflate0:amd64 1.10-2
libfontconfig1:amd64 2.13.1-4.2ubuntu5

Reinstalled:
logwatch:amd64 7.5.6-1ubuntu1

Removed:
libdate-manip-perl:all 6.86-1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1

Purged:
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1

----- dpkg status changes End -----

----- Disk Space Begin -----

Filesystem      Size  Used Avail Use% Mounted on
rootfs          183G  144G   40G  79% /
C:\              183G  144G   40G  79% /mnt/c
D:\              293G  174G  120G  60% /mnt/d

----- Disk Space End -----

##### Logwatch End #####
```

```
aryan@LAPTOP-S7MB25C9: ~/report
linux-libc-dev:amd64 5.15.0-60.66
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
manpages-dev:all 5.10-1ubuntu1
postfix:amd64 3.6.4-1ubuntu1
rcs:amd64 5.10.1-1
rpcsvc-proto:amd64 1.4.2-0ubuntu6
rsyslog-gnutls:amd64 8.2112.0-2ubuntu2.2
ssl-cert:all 1.1.2

Reinstalled:
logwatch:amd64 7.5.6-1ubuntu1

Removed:
libdate-manip-perl:all 6.86-1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1

Purged:
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1
logwatch:amd64 7.5.6-1ubuntu1

----- dpkg status changes End -----

----- Disk Space Begin -----

Filesystem      Size  Used Avail Use% Mounted on
rootfs          183G  144G   40G  79% /
C:\              183G  144G   40G  79% /mnt/c
D:\              293G  174G  120G  60% /mnt/d

----- Disk Space End -----

##### Logwatch End #####
```

9<sup>th</sup> April

```
aryan@LAPTOP-S7MB25C9: ~/report
aryan@LAPTOP-S7MB25C9:~/report$ sudo logwatch --range 'between -90 days and today'

##### Logwatch 7.5.6 (07/23/21) #####
Processing Initiated: Sun Apr  9 22:35:12 2023
Date Range Processed: between -90 days and today
                     ( 2023-Jan-09 / 2023-Apr-09 )
Period is day.
Detail Level of Output: 0
Type of Output/Format: stdout / text
Logfiles for Host: LAPTOP-S7MB25C9
#####

----- dpkg status changes Begin -----

Installed:
bc:amd64 1.07.1-3build1
cpp-11:amd64 11.3.0-1ubuntu1~22.04
cpp:amd64 4:11.2.0-1ubuntu1
fontconfig-config:all 2.13.1-4.2ubuntu5
fonts-dejavu-core:all 2.37-2build1
foremost:amd64 1.5.7-11
gcc-11-base:amd64 11.3.0-1ubuntu1~22.04
gcc-11:amd64 11.3.0-1ubuntu1~22.04
gcc:amd64 4:11.2.0-1ubuntu1
gdb:amd64 12.1-0ubuntu1~22.04
hwinfo:amd64 21.72-1
libasan6:amd64 11.3.0-1ubuntu1~22.04
libatomic1:amd64 12.1.0-2ubuntu1~22.04
libbabeltrace1:amd64 1.5.8-2build1
libboost-regex1.74.0:amd64 1.74.0-14ubuntu3
libc-dev-bin:amd64 2.35-0ubuntu3.1
libc-devtools:amd64 2.35-0ubuntu3.1
libc6-dbg:amd64 2.35-0ubuntu3.1
libc6-dev:amd64 2.35-0ubuntu3.1
libcc1-0:amd64 12.1.0-2ubuntu1~22.04
libcrypt-dev:amd64 1:4.4.27-1
libdate-manip-perl:all 6.86-1
libdate-manip-perl:all 6.86-1
libdebuginfod-common:all 0.186-1build1
libdebuginfod1:amd64 0.186-1build1
libdeflate0:amd64 1.10-2

----- dpkg status changes End -----

----- Disk Space Begin -----

Filesystem      Size  Used Avail Use% Mounted on
rootfs          183G  147G   37G   80% /
C:\              183G  147G   37G   80% /mnt/c
D:\              293G  174G  120G   60% /mnt/d

----- Disk Space End -----

##### Logwatch End #####
```

```
aryan@LAPTOP-S7MB25C9: ~/report
logwatch:all 7.5.6-1ubuntu1
logwatch:all 7.5.6-1ubuntu1
logwatch:all 7.5.6-1ubuntu1
manpages-dev:all 5.10-1ubuntu1
postfix:amd64 3.6.4-1ubuntu1
rcs:amd64 5.10.1-1
rpcsvc-proto:amd64 1.4.2-0ubuntu6
rsyslog-gnutls:amd64 8.2112.0-2ubuntu2.2
scalpel:amd64 1.60-9
ssl-cert:all 1.1.2

Reinstalled:
logwatch:all 7.5.6-1ubuntu1

Removed:
libdate-manip-perl:all 6.86-1
logwatch:all 7.5.6-1ubuntu1
logwatch:all 7.5.6-1ubuntu1
logwatch:all 7.5.6-1ubuntu1

Purged:
logwatch:all 7.5.6-1ubuntu1
logwatch:all 7.5.6-1ubuntu1
logwatch:all 7.5.6-1ubuntu1

----- dpkg status changes End -----

----- Disk Space Begin -----

Filesystem      Size  Used Avail Use% Mounted on
rootfs          183G  147G   37G   80% /
C:\              183G  147G   37G   80% /mnt/c
D:\              293G  174G  120G   60% /mnt/d

----- Disk Space End -----

##### Logwatch End #####
```



## **4. Reference**

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

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