INT 301: OPEN-SOURCE TECHNOLOGIES

A REPORT

Submitted in partial fulfillment of the requirements of the award of the degree of

Bachelor of Technology

Computer Science Engineering (Hons.)

Lovely Professional University

Phagwara, Punjab.

Submitted by:

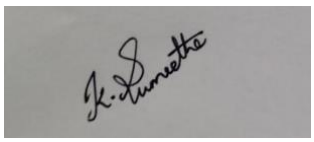
Name: Kota Sumeetha

Reg Number: 11901942

Section: KE059

Roll no: 34.

Signature of the student



Submitted to:

Name: Manpreet Singh

Use any open source software to generate your entire system's log report of past 3 months along with this find partial and full multimedia files(video files) in DataStream.

Open-source technologies refer to software, hardware and other technological solutions whose source code or design is publicly available for anyone to view, modify and distribute. There are people or group of people who develop and contribute to it.

Some examples of opensource software are

- Linux
- Github
- Apache
- MySQL
- Ruby on Rails
- Wordpress
- Hadoop etc…

Advantages of Opensource technologies

1) Affordability
2) Transparency
3) Flexibility
4) Security
5) Innovation
6) Collaboration etc…

Disadvantages of Opensource technologies

1) Security risks
2) Compatible issues
3) Poor developer practices
4) Lack of warranties
5) Hidden costs etc…

Use any open-source software to generate your entire system's log report of past 3 months

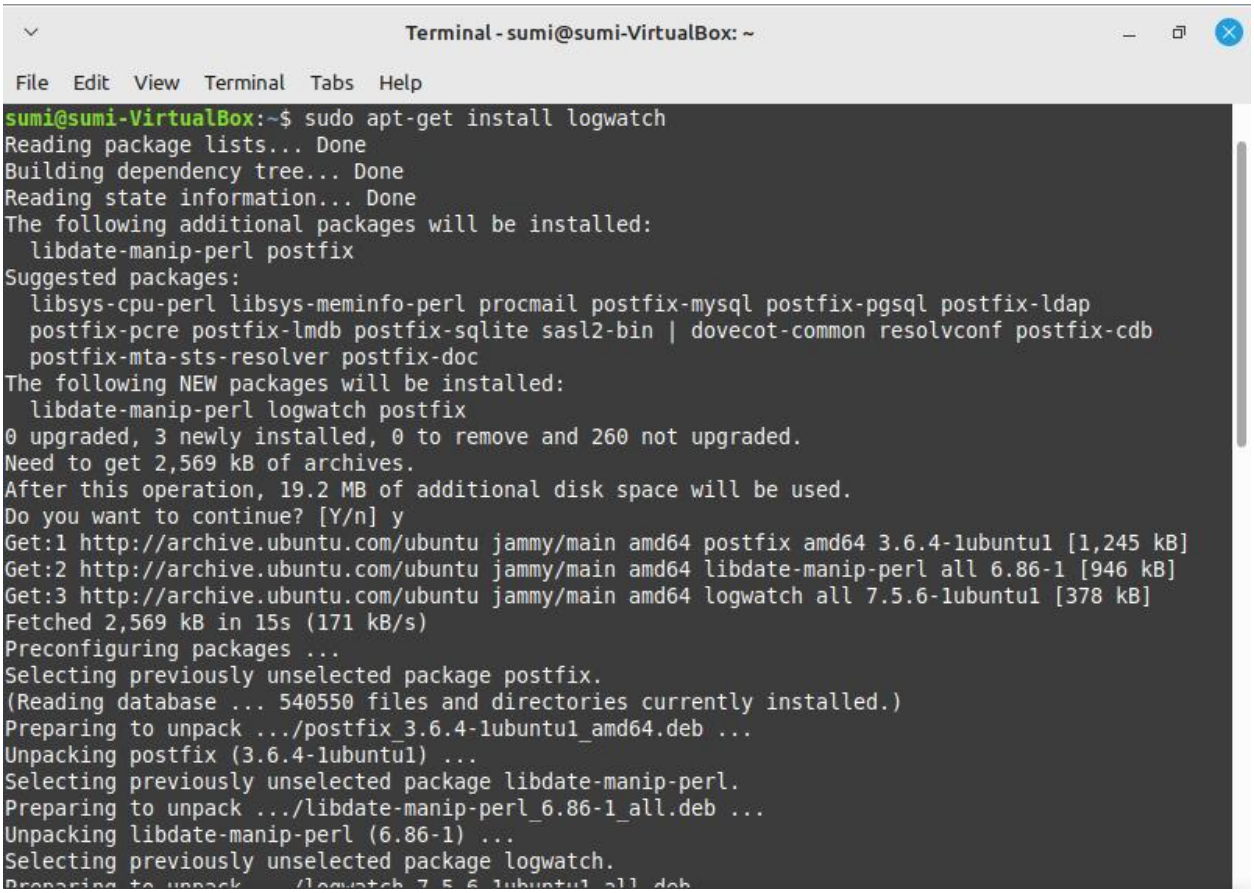
There are many open source softwares that will help like Logrotate, Logwatch, Graylog etc…

Here I used Logwatch to generate the log report.

Logwatch: Logwatch is a powerful and versatile log parser and analyzer. It is a customizable, pluggable log-monitoring system. Logwatch is designed to give a unified report of all activity on a server, which can be delivered through the command line or email.

To generate a systems log report we first need to install logwatch.

Command used to install logwatch: **Sudo apt-get install logwatch**



Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

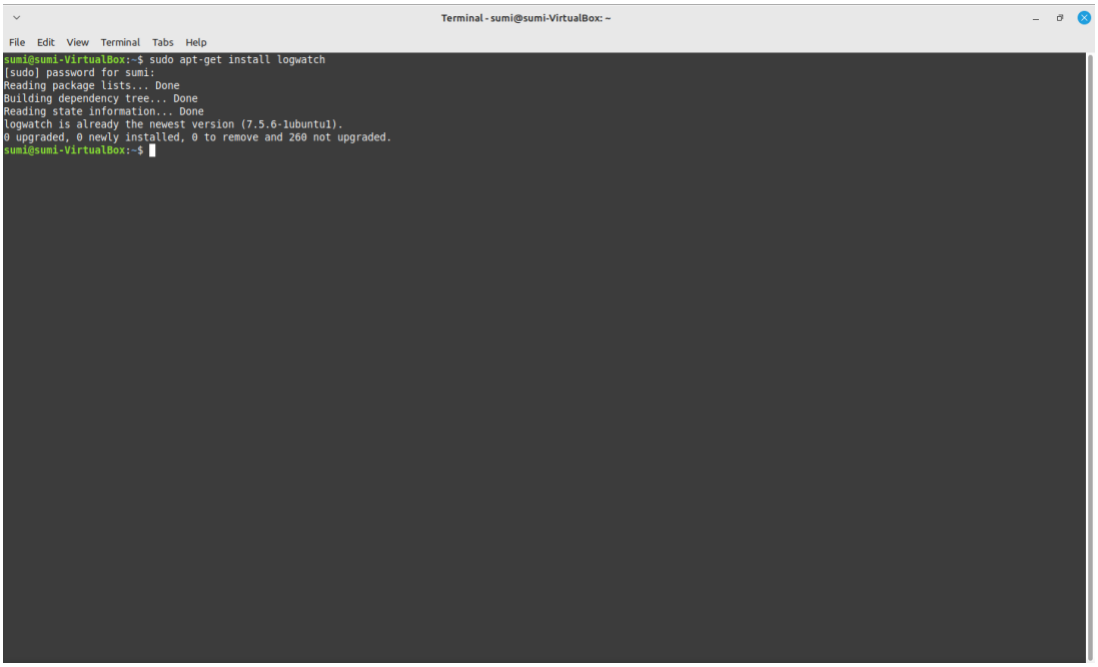
```
Selecting previously unselected package postfix.
(Reading database ... 540550 files and directories currently installed.)
Preparing to unpack .../postfix_3.6.4-1ubuntu1_amd64.deb ...
Unpacking postfix (3.6.4-1ubuntu1) ...
Selecting previously unselected package libdate-manip-perl.
Preparing to unpack .../libdate-manip-perl_6.86-1_all.deb ...
Unpacking libdate-manip-perl (6.86-1) ...
Selecting previously unselected package logwatch.
Preparing to unpack .../logwatch_7.5.6-1ubuntu1_all.deb ...
Unpacking logwatch (7.5.6-1ubuntu1) ...
Setting up postfix (3.6.4-1ubuntu1) ...
Adding group `postfix' (GID 139) ...
Done.
Adding system user `postfix' (UID 129) ...
Adding new user `postfix' (UID 129) with group `postfix' ...
Not creating home directory `/var/spool/postfix'.
Creating /etc/postfix/dynamicmaps.cf
Adding group `postdrop' (GID 140) ...
Done.
setting myhostname: sumi-VirtualBox.lpu.com
setting alias maps
setting alias database
mailname is not a fully qualified domain name.  Not changing /etc/mailname.
setting destinations: $myhostname, sumi-VirtualBox, localhost.localdomain, , localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
setting myhostname: sumi-VirtualBox.lpu.com
setting alias maps
setting alias database
mailname is not a fully qualified domain name.  Not changing /etc/mailname.
setting destinations: $myhostname, sumi-VirtualBox, localhost.localdomain, , localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
/etc/aliases does not exist, creating it.
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with a default configuration.  If you need to
make changes, edit /etc/postfix/main.cf (and others) as needed.  To view
Postfix configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /lib/systemd/system/
postfix.service.
Setting up libdate-manip-perl (6.86-1) ...
Setting up logwatch (7.5.6-1ubuntu1) ...
Processing triggers for ufw (0.36.1-4build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for rsyslog (8.2112.0-2ubuntu2.2) ...
sumi@sumi-VirtualBox:~$
```

After installing you will get logwatch like this!



To view the Logwatch report on the command line, use the following command:

For current day – **sudo logwatch**

For last one week **– sudo logwatch --range 'between -7 days and today'**

Here, --range option is helpful to get a report for the specific date range. It is generally followed by a date range specification.

For our project, we need a log report of past 3 months which is approximately 90 days.

So the command we need to generate log report is

sudo logwatch –range 'between -30 days and today'

And with this command we get a result like this,

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

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

sumi@sumi-VirtualBox:~$ sudo logwatch --range 'between -90 days and today'

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Fri Apr  7 15:47:26 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: sumi-VirtualBox
 ##################################################################

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

 Installed:
    arduino-builder:amd64 1.3.25-3
    arduino-core-avr:all 1.8.4+dfsg1-1
    arduino-ctags:amd64 5.8-arduino11-1
    arduino:amd64 2:1.8.19+dfsg1-1
    avr-libc:all 1:2.0.0+Atmel3.6.2-3
    avrdude:amd64 6.3-20171130+svn1429-2
    binutils-avr:amd64 2.26.20160125+Atmel3.6.2-4
    extra-xdg-menus:all 1.0-6
    g++-11:amd64 11.3.0-1ubuntu1~22.04
    g++:amd64 4:11.2.0-1ubuntu1
    gcc-avr:amd64 1:5.4.0+Atmel3.6.2-3
    gedit-common:all 41.0-3
    gedit:amd64 41.0-3
    gnome-system-monitor:amd64 42.0-1
    java-wrappers:all 0.3
    libapache-pom-java:all 18-1
    libastylej-jni:amd64 3.1-2build1
    libbatik-java:all 1.14-1
    libbcpg-java:all 1.68-5
    libbcprov-java:all 1.68-5
    libc-dev-bin:amd64 2.35-0ubuntu3.1
    libc-devtools:amd64 2.35-0ubuntu3.1
    libc6-dev:amd64 2.35-0ubuntu3.1
    libcommons-codec-java:all 1.15-1
    libcommons-compress-java:all 1.21-1
    libcommons-exec-java:all 1.3-2
    libcommons-io-java:all 2.11.0-2
    libcommons-lang3-java:all 3.11-1
    libcommons-logging-java:all 1.2-2
    libcommons-net-java:all 3.6-1
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
    libcommons-codec-java:all 1.15-1
    libcommons-compress-java:all 1.21-1
    libcommons-exec-java:all 1.3-2
    libcommons-io-java:all 2.11.0-2
    libcommons-lang3-java:all 3.11-1
    libcommons-logging-java:all 1.2-2
    libcommons-net-java:all 3.6-1
    libcommons-parent-java:all 43-1
    libcrypt-dev:amd64 1:4.4.27-1
    libdate-manip-perl:all 6.86-1
    libftdi1:amd64 0.20-4ubuntu1
    libgoogle-gson-java:all 2.8.8-1
    libhidapi-libusb0:amd64 0.11.2-1
    libhttpclient-java:all 4.5.13-3
    libhttpcore-java:all 4.4.14-2
    libjackson2-annotations-java:all 2.13.0-1
    libjackson2-core-java:all 2.13.0-2
    libjackson2-databind-java:all 2.13.0-2
    libjaxp1.3-java:all 1.3.05-6
    libjmdns-java:all 3.5.5-1
    libjna-java:all 5.9.0-1
    libjna-jni:amd64 5.9.0-1
    libjna-platform-java:all 5.9.0-1
    libjsch-java:all 0.1.55-1
    libjssc-java:amd64 2.8.0-3
    libjzlib-java:all 1.1.3-2
    liblightcouch-java:all 0.0.6-1.1
    liblistserialsj-dev:amd64 1.4.0-1ubuntu0.22.04.1
    liblistserialsj1:amd64 1.4.0-1ubuntu0.22.04.1
    liblog4j2-java:all 2.17.1-1
    libmongodb-java:all 3.6.3-2
    libnsl-dev:amd64 1.3.0-2build2
    librsyntaxtextarea-java:all 2.5.8-1
    librxtx-java:amd64 2.2pre2+dfsg1-2
    libsemver-java:all 0.9.0-4
    libserialport0:amd64 0.1.1-4
    libslf4j-java:all 1.7.32-1
    libstdc++-11-dev:amd64 11.3.0-1ubuntu1~22.04
    libtirpc-dev:amd64 1.3.2-2ubuntu0.1
    libusb-0.1-4:amd64 2:0.1.12-32build3
    libxalan2-java:all 2.7.2-4
    libxerces2-java:all 2.12.1-1
    libxml-commons-external-java:all 1.4.01-5
    libxml-commons-resolver1.1-java:all 1.2-11
    libxmlgraphics-commons-java:all 2.6-1
    logwatch:all 7.5.6-1ubuntu1
    postfix:amd64 3.6.4-1ubuntu1
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
   libxalan2-java:all 2.7.2-4
   libxerces2-java:all 2.12.1-1
   libxml-commons-external-java:all 1.4.01-5
   libxml-commons-resolver1.1-java:all 1.2-11
   libxmlgraphics-commons-java:all 2.6-1
   logwatch:all 7.5.6-1ubuntu1
   postfix:amd64 3.6.4-1ubuntu1
   rcs:amd64 5.10.1-1
   rpcsvc-proto:amd64 1.4.2-0ubuntu6

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


-------------------- Kernel Begin -----------------------


WARNING:  Kernel Errors Present
   WARNING: Spectre v2 mitigation leaves CPU vulner ...:  20 Time(s)
   [drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send  ...:  20 Time(s)

---------------------- Kernel End ------------------------


-------------------- pam_unix Begin -----------------------

lightdm:
   Unknown Entries:
      session opened for user sumi(uid=1000) by (uid=0): 20 Time(s)
      authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=  user=sumi: 4 Time(s)
      authentication failure; logname= uid=0 euid=0 tty=:1 ruser= rhost=  user=sumi: 2 Time(s)
      session closed for user sumi: 1 Time(s)

lightdm-greeter:
   Unknown Entries:
      session opened for user lightdm(uid=113) by (uid=0): 70 Time(s)
      session closed for user lightdm: 6 Time(s)

login:
   Authentication Failures:
      unknown (): 2 Time(s)
      sumi (): 1 Time(s)
   Invalid Users:
      Unknown Account: 2 Time(s)

su-l:
   Authentication Failures:
      sumi(1000) -> root: 7 Time(s)
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
      sumi (): 1 Time(s)
   Invalid Users:
      Unknown Account: 2 Time(s)

su-l:
   Authentication Failures:
      sumi(1000) -> root: 7 Time(s)

sudo:
   Sessions Opened:
      sumi -> root(uid=0): 81 Time(s)


---------------------- pam_unix End ------------------------


-------------------- Postfix Begin -----------------------

  14.635K  Bytes accepted                              14,986
  20.059K  Bytes delivered                             20,540
========   ==============================================

       4   Accepted                                   100.00%
--------   ----------------------------------------------
       4   Total                                      100.00%
========   ==============================================

       6   Removed from queue                              6
       4   Delivered                                       4
       2   Bounced (remote)                                2
       2   Notifications sent                              2

       1   Connection failures (outbound)                  1

       4   Postfix start                                   4
       4   Postfix refresh                                 4


---------------------- Postfix End ------------------------


-------------------- Connections (secure-log) Begin -----------------------

New Users:
   postfix (129)

New Groups:
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
-------------------- Connections (secure-log) Begin -----------------------

New Users:
   postfix (129)

New Groups:
   postfix (139)
   postdrop (140)


Changed users password:
   postfix changed password: 1 Time(s)

Errors:
   Service su:
      FAILED SU (to root) sumi on pts/0: 4 Time(s)
      FAILED SU (to root) sumi on pts/1: 3 Time(s)

Changed password expiry for users:
   postfix : 1 Time(s)

**Unmatched Entries**
   dbus-daemon: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms): 87 Time(s)
   gnome-keyring-daemon: couldn't access control socket: /run/user/1000/keyring/control: No such file or directory: 15 Time(s)
   lightdm: gkr-pam: gnome-keyring-daemon started properly: 70 Time(s)
   lightdm: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring: 20 Time(s)
   lightdm: gkr-pam: stashed password to try later in open session: 61 Time(s)
   lightdm: gkr-pam: unable to locate daemon control file: 61 Time(s)
   lightdm: pam_succeed_if(lightdm:auth): requirement "user ingroup nopasswdlogin" not met by user "sumi": 76 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure: 2 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'sumi', Authentication failure: 1 Time(s)
   systemd-logind: Session c2 logged out. Waiting for processes to exit.: 1 Time(s)
   systemd-logind: System is powering down.: 1 Time(s)

---------------------- Connections (secure-log) End ------------------------


-------------------- Sudo (secure-log) Begin -----------------------


sumi => root
------------
/usr/bin/apt-get                -   5 Time(s).
/usr/bin/mint-refresh-cache     -  20 Time(s).
/usr/lib/linuxmint/mintUpdate/dpkg_lock_check.sh -  34 Time(s).
/usr/local/bin/apt              -  10 Time(s).
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure: 2 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'sumi', Authentication failure: 1 Time(s)
   systemd-logind: Session c2 logged out. Waiting for processes to exit.: 1 Time(s)
   systemd-logind: System is powering down.: 1 Time(s)

---------------------- Connections (secure-log) End ------------------------


-------------------- Sudo (secure-log) Begin -----------------------


sumi => root
------------
/usr/bin/apt-get                -   5 Time(s).
/usr/bin/mint-refresh-cache     -  20 Time(s).
/usr/lib/linuxmint/mintUpdate/dpkg_lock_check.sh -  34 Time(s).
/usr/local/bin/apt              -  10 Time(s).
/usr/sbin/logwatch              -  12 Time(s).

---------------------- Sudo (secure-log) End ------------------------


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

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        24G   11G   13G  46% /
/dev/sda2       512M  5.3M  507M   2% /boot/efi


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


-------------------- lm_sensors output Begin -----------------------

BAT0-acpi-0
Adapter: ACPI interface
in0:          10.00 V


---------------------- lm_sensors output End ------------------------


###################### Logwatch End ########################

sumi@sumi-VirtualBox:~$ sudo logwatch --range 'between -90 days and today' > 3monthsreport.txt
sumi@sumi-VirtualBox:~$ ls
'!'                 A        apple    cal.c        d1        Documents   f2          fileexists   if                  'm*'         OR         Stringeq   switchq     Videos
```

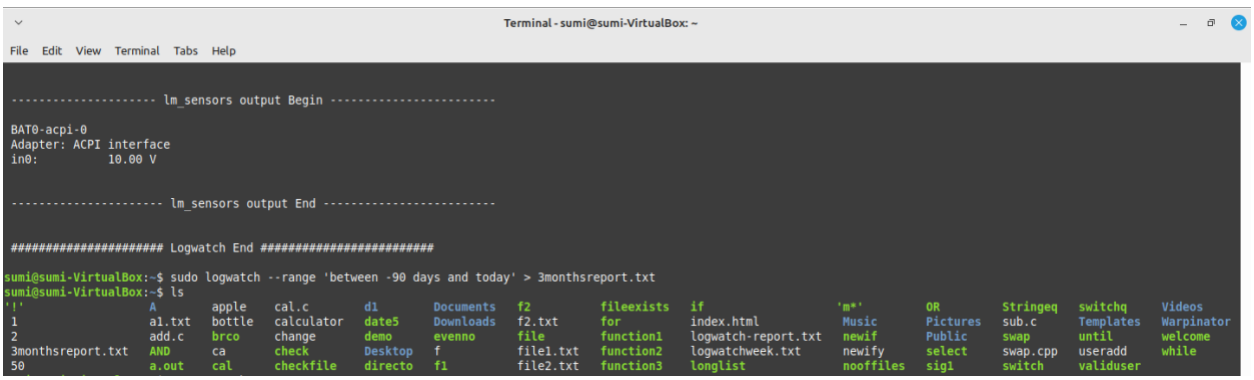
So this is the log report of past 3 months that we intended to find. As we can see the result directly here, there are also other ways to view this result. Like,

1) We can redirect this log report to a file in our system.
2) We can send this log report to our own email address.

Redirecting this log report to a file in our system:

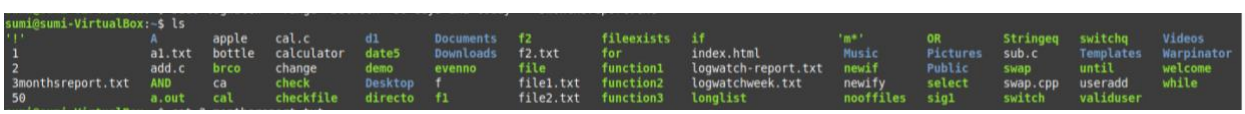
So command to redirect this log report to a file is,

sudo logwatch –range 'between -30 days and today' > 3monthsreport.txt



As we know that with the help of **ls** command, we can view all the files, we can also view this file called 3monthsreport.txt in the list obtained from ls command. So the file that we created to redirect the log report is created.

Result looks like this,



So, we can find the 3monthsreport.txt above in the list as mentioned. Now as we are redirecting our report to this file, we have to view this file to see the contents inside. The general command to view any file is cat. With the help of cat command we can view content of the files.

So, Command to view this file is,

cat 3monthsreport.txt

And the result will be something like this,

```
Terminal - sumi@sumi-VirtualBox: ~
File  Edit  View  Terminal  Tabs  Help
 50                a.out    cal      checkfile    directo   f1          file2.txt   function3    longlist             nooffiles   sig1       switch     validuser
sumi@sumi-VirtualBox:~$ cat 3 monthsreport.txt
cat: 3: No such file or directory
cat: monthsreport.txt: No such file or directory
sumi@sumi-VirtualBox:~$ cat 3monthsreport.txt

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Fri Apr  7 15:48:48 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: sumi-VirtualBox
 ##################################################################

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

 Installed:
    arduino-builder:amd64 1.3.25-3
    arduino-core-avr:all 1.8.4+dfsg1-1
    arduino-ctags:amd64 5.8-arduino11-1
    arduino:amd64 2:1.8.19+dfsg1-1
    avr-libc:all 1:2.0.0+Atmel3.6.2-3
    avrdude:amd64 6.3-20171130+svn1429-2
    binutils-avr:amd64 2.26.20160125+Atmel3.6.2-4
    extra-xdg-menus:all 1.0-6
    g++-11:amd64 11.3.0-1ubuntu1~22.04
    g++:amd64 4:11.2.0-1ubuntu1
    gcc-avr:amd64 1:5.4.0+Atmel3.6.2-3
    gedit-common:all 41.0-3
    gedit:amd64 41.0-3
    gnome-system-monitor:amd64 42.0-1
    java-wrappers:all 0.3
    libapache-pom-java:all 18-1
    libastylej-jni:amd64 3.1-2build1
    libbatik-java:all 1.14-1
    libbcpg-java:all 1.68-5
    libbcprov-java:all 1.68-5
    libc-dev-bin:amd64 2.35-0ubuntu3.1
    libc-devtools:amd64 2.35-0ubuntu3.1
    libc6-dev:amd64 2.35-0ubuntu3.1
    libcommons-codec-java:all 1.15-1
    libcommons-compress-java:all 1.21-1
    libcommons-exec-java:all 1.3-2
    libcommons-io-java:all 2.11.0-2
    libcommons-lang3-java:all 3.11-1
```

```
Terminal - sumi@sumi-VirtualBox: ~
File  Edit  View  Terminal  Tabs  Help
    libcommons-io-java:all 2.11.0-2
    libcommons-lang3-java:all 3.11-1
    libcommons-logging-java:all 1.2-2
    libcommons-net-java:all 3.6-1
    libcommons-parent-java:all 43-1
    libcrypt-dev:amd64 1:4.4.27-1
    libdate-manip-perl:all 6.86-1
    libftdi1:amd64 0.20-4ubuntu1
    libgoogle-gson-java:all 2.8.8-1
    libhidapi-libusb0:amd64 0.11.2-1
    libhttpclient-java:all 4.5.13-3
    libhttpcore-java:all 4.4.14-2
    libjackson2-annotations-java:all 2.13.0-1
    libjackson2-core-java:all 2.13.0-2
    libjackson2-databind-java:all 2.13.0-2
    libjaxp1.3-java:all 1.3.05-6
    libjmdns-java:all 3.5.5-1
    libjna-java:all 5.9.0-1
    libjna-jni:amd64 5.9.0-1
    libjna-platform-java:all 5.9.0-1
    libjsch-java:all 0.1.55-1
    libjssc-java:amd64 2.8.0-3
    libjzlib-java:all 1.1.3-2
    liblightcouch-java:all 0.0.6-1.1
    liblistserialsj-dev:amd64 1.4.0-1ubuntu0.22.04.1
    liblistserialsj1:amd64 1.4.0-1ubuntu0.22.04.1
    liblog4j2-java:all 2.17.1-1
    libmongodb-java:all 3.6.3-2
    libnsl-dev:amd64 1.3.0-2build2
    librsyntaxtextarea-java:all 2.5.8-1
    librxtx-java:amd64 2.2pre2+dfsg1-2
    libsemver-java:all 0.9.0-4
    libserialport0:amd64 0.1.1-4
    libslf4j-java:all 1.7.32-1
    libstdc++-11-dev:amd64 11.3.0-1ubuntu1~22.04
    libtirpc-dev:amd64 1.3.2-2ubuntu0.1
    libusb-0.1-4:amd64 2:0.1.12-32build3
    libxalan2-java:all 2.7.2-4
    libxerces2-java:all 2.12.1-1
    libxml-commons-external-java:all 1.4.01-5
    libxml-commons-resolver1.1-java:all 1.2-11
    libxmlgraphics-commons-java:all 2.6-1
    logwatch:all 7.5.6-1ubuntu1
    postfix:amd64 3.6.4-1ubuntu1
    rcs:amd64 5.10.1-1
    rpcsvc-proto:amd64 1.4.2-0ubuntu6
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
   libxml-commons-resolver1.1-java:all 1.2-11
   libxmlgraphics-commons-java:all 2.6-1
   logwatch:all 7.5.6-1ubuntu1
   postfix:amd64 3.6.4-1ubuntu1
   rcs:amd64 5.10.1-1
   rpcsvc-proto:amd64 1.4.2-0ubuntu6

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


-------------------- Kernel Begin ------------------------


WARNING:  Kernel Errors Present
   WARNING: Spectre v2 mitigation leaves CPU vulner ...:  20 Time(s)
   [drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send  ...:  20 Time(s)

--------------------- Kernel End ------------------------


-------------------- pam_unix Begin ------------------------

lightdm:
   Unknown Entries:
      session opened for user sumi(uid=1000) by (uid=0): 20 Time(s)
      authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost=  user=sumi: 4 Time(s)
      authentication failure; logname= uid=0 euid=0 tty=:1 ruser= rhost=  user=sumi: 2 Time(s)
      session closed for user sumi: 1 Time(s)

lightdm-greeter:
   Unknown Entries:
      session opened for user lightdm(uid=113) by (uid=0): 70 Time(s)
      session closed for user lightdm: 6 Time(s)

login:
   Authentication Failures:
      unknown (): 2 Time(s)
      sumi (): 1 Time(s)
   Invalid Users:
      Unknown Account: 2 Time(s)

su-l:
   Authentication Failures:
      sumi(1000) -> root: 7 Time(s)

sudo:
   Sessions Opened:
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
su-l:
   Authentication Failures:
      sumi(1000) -> root: 7 Time(s)

sudo:
   Sessions Opened:
      sumi -> root(uid=0): 82 Time(s)


--------------------- pam_unix End ------------------------


-------------------- Postfix Begin ------------------------

  14.635K  Bytes accepted                              14,986
  20.059K  Bytes delivered                             20,540
========   ==============================================

       4   Accepted                                   100.00%
--------   ----------------------------------------------
       4   Total                                      100.00%
========   ==============================================

       6   Removed from queue                              6
       4   Delivered                                       4
       2   Bounced (remote)                                2
       2   Notifications sent                              2

       1   Connection failures (outbound)                  1

       4   Postfix start                                   4
       4   Postfix refresh                                 4


--------------------- Postfix End ------------------------


-------------------- Connections (secure-log) Begin ------------------------

New Users:
   postfix (129)

New Groups:
   postfix (139)
   postdrop (140)
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
New Users:
   postfix (129)

New Groups:
   postfix (139)
   postdrop (140)


Changed users password:
   postfix changed password: 1 Time(s)

Errors:
   Service su:
      FAILED SU (to root) sumi on pts/0: 4 Time(s)
      FAILED SU (to root) sumi on pts/1: 3 Time(s)

Changed password expiry for users:
   postfix : 1 Time(s)

**Unmatched Entries**
   dbus-daemon: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms): 87 Time(s)
   gnome-keyring-daemon: couldn't access control socket: /run/user/1000/keyring/control: No such file or directory: 15 Time(s)
   lightdm: gkr-pam: gnome-keyring-daemon started properly: 70 Time(s)
   lightdm: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring: 20 Time(s)
   lightdm: gkr-pam: stashed password to try later in open session: 61 Time(s)
   lightdm: gkr-pam: unable to locate daemon control file: 61 Time(s)
   lightdm: pam_succeed_if(lightdm:auth): requirement "user ingroup nopasswdlogin" not met by user "sumi": 76 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure: 2 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'sumi', Authentication failure: 1 Time(s)
   systemd-logind: Session c2 logged out. Waiting for processes to exit.: 1 Time(s)
   systemd-logind: System is powering down.: 1 Time(s)

--------------------- Connections (secure-log) End ------------------------


--------------------- Sudo (secure-log) Begin ------------------------


sumi => root
------------
/usr/bin/apt-get                -   5 Time(s).
/usr/bin/mint-refresh-cache     -  20 Time(s).
/usr/lib/linuxmint/mintUpdate/dpkg_lock_check.sh -  34 Time(s).
/usr/local/bin/apt              -  10 Time(s).
/usr/sbin/logwatch              -  13 Time(s).

--------------------- Sudo (secure-log) End ------------------------
```

Terminal - sumi@sumi-VirtualBox: ~

File Edit View Terminal Tabs Help

```
   lightdm: gkr-pam: unable to locate daemon control file: 61 Time(s)
   lightdm: pam_succeed_if(lightdm:auth): requirement "user ingroup nopasswdlogin" not met by user "sumi": 76 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure: 2 Time(s)
   login: FAILED LOGIN (1) on '/dev/tty1' FOR 'sumi', Authentication failure: 1 Time(s)
   systemd-logind: Session c2 logged out. Waiting for processes to exit.: 1 Time(s)
   systemd-logind: System is powering down.: 1 Time(s)

--------------------- Connections (secure-log) End ------------------------


--------------------- Sudo (secure-log) Begin ------------------------


sumi => root
------------
/usr/bin/apt-get                -   5 Time(s).
/usr/bin/mint-refresh-cache     -  20 Time(s).
/usr/lib/linuxmint/mintUpdate/dpkg_lock_check.sh -  34 Time(s).
/usr/local/bin/apt              -  10 Time(s).
/usr/sbin/logwatch              -  13 Time(s).

--------------------- Sudo (secure-log) End ------------------------


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

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        24G   11G   13G  46% /
/dev/sda2       512M  5.3M  507M   2% /boot/efi


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


--------------------- lm_sensors output Begin ------------------------

BAT0-acpi-0
Adapter: ACPI interface
in0:          10.00 V


--------------------- lm_sensors output End ------------------------


###################### Logwatch End #########################

sumi@sumi-VirtualBox:~$
```

Redirecting this log report to a file in our own email address:

You may need to install a mail transfer agent (MTA) such as Postfix or Sendmail and configure it to send email from the command line.

Mail transfer agent:

A mail transfer agent (MTA) is software that transfers emails between computers of a sender and a recipient. MTAs use a store-and-forward model of mail handling and can impact email deliverability by protecting and strengthening the sender's reputation. MTAs are considered a mail server and work with other components in the message handling system to enable the email delivery process, receiving emails etc.…

Examples of MTAs: Exim, Postfix, Sendmail, Qmail, Microsoft Exchange Server, and Oracle Beehive

In my work I used Postfix as a MTA,

Postfix: Postfix is a popular open-source mail transfer agent (MTA) that is used to route and deliver email messages on Linux and Unix systems. Postfix is known for its security, performance, and flexibility, and is used by many organizations as their primary mail server.

Overall, Postfix is a reliable and popular choice for organizations looking for a flexible and secure mail server solution.

First, we need to update the package manager to do this installation.

Command to update the package manager,

sudo apt-get update

```
sumi@sumi-VirtualBox:~$ sudo apt-get update
[sudo] password for sumi:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Ign:5 http://packages.linuxmint.com vera InRelease
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [41.4 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [18.5 kB]
Hit:8 http://packages.linuxmint.com vera Release
Fetched 397 kB in 2s (180 kB/s)

Reading package lists... Done
```

Now we need to install Postfix,

Command to install postfix is,

sudo apt-get install postfix

```
sumi@sumi-VirtualBox:~$ sudo apt-get install postfix
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
postfix is already the newest version (3.6.4-1ubuntu1).
postfix set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 260 not upgraded.
```

To check if we successfully installed postfix,

Command is,

sudo systemctl status postfix

```
sumi@sumi-VirtualBox:~$ sudo systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
     Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
     Active: active (exited) since Fri 2023-04-07 15:16:51 IST; 2h 27min ago
       Docs: man:postfix(1)
    Process: 1492 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1492 (code=exited, status=0/SUCCESS)
        CPU: 6ms

Apr 07 15:16:51 sumi-VirtualBox systemd[1]: Starting Postfix Mail Transport Agent...
Apr 07 15:16:51 sumi-VirtualBox systemd[1]: Finished Postfix Mail Transport Agent.
```

So, postfix is installed and is active.

Now run the following code to send the report to your email address,

sudo logwatch --detail High --range 'between -90 days and today' –mailto -s "Logwatch report" sumeethakota@gmail.com

breaking down the above code :

logwatch – opensource software that we are using

--detail High – Gives High-level detail

--range – Indicates the specific date range

--mailto – helpful to send mail to specific mail address

This command will generate a Logwatch report for the past 3months with high-level detail and send it to the email address sumeethakota@gmail.com with the subject "Logwatch Report".

Another way of doing it is,

going into the configuration file of logwatch and giving mail addresses, Like

1) Installing postfix
2) Going to configuration file like /etc/logwatch/conf/logwatch.conf
3) Locate the MailTo in the configuration file
   Uncomment it and give your mail address –
   MailTo = sumeethakota@gmail.com
4) Save and close this file
5) Now, run logwatch and write the following command to send the report to email address

   logwatch 3monthsreport.txt --mailto sumeethakota@gmail.com

   So, this is how we use open source software to generate your entire system's log report of past 3 months

Find partial and full multimedia files(video files) in DataStream.

The "partial" and "full" are primarily used to describe media types and screen captures rather than multimedia files themselves.

Full media type - It is one that fully defines the format of the media stream like, full-screen screenshot gives full image of screen.

Partial media type – It lacks one or more attributes needed for a complete media type like, Partial screen shot capture only partial records of a specific area of the screen.

It is difficult to describe whether a file is full or partial multimedia file, But with the help of tools like foremost, we can recover the damaged and corrupted multimedia files and with the help of data received we can find if it is full or partial multimedia file.

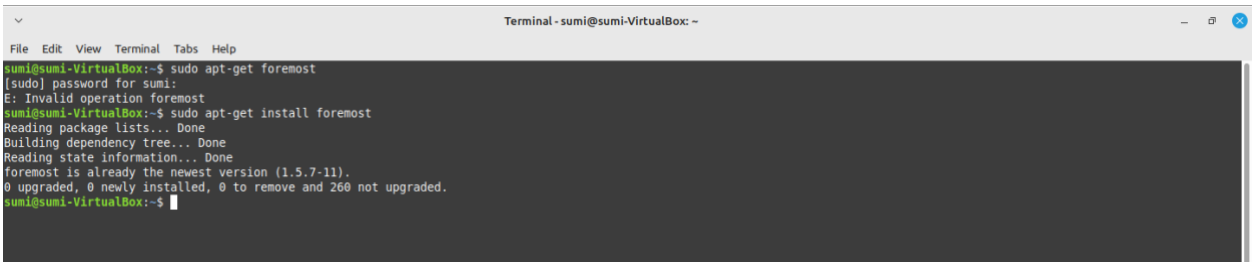
Foremost-

Foremost is a powerful digital forensics tool that can be used to recover multimedia files from damaged or corrupted storage media. When using Foremost, you can generate a report that provides detailed information about the recovered files, including their size, type, and location.

Foremost can recover entire files or partial file fragments from damaged disks and deleted files on a hard drive. It can read data from the actual physical media, entire drive image files, and file headers and data from images created via the Linux/Unix "dd" command.

The program can recover specific file types, including jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, and cpp. It can be used via the command-line interface and is a simple and effective tool for data recovery.

For this, we need to first install Foremost in our system,



This shows us that the foremost is successfully installed in our system.

Now I initially created a directory named as Datastream in my system, with the help of ls command we can view this file.

Datastream

Command to create a datastream:

First create a text file named myfile.txt,

Sudo setfattr -n user.mystream -v “Hello Worls!” myfile.txt

Command to view this datastream:

Sudo getfattr -n user.mystream myfile.txt

Output will be something like this,

User.mystream=”Hello Worls!”

```
sumi@sumi-VirtualBox:~$ ls
3monthsreport.txt  Datastream  Desktop  Documents  Downloads  logwatch-report.txt  logwatchweek.txt  Music  Pictures  Public  Templates  Videos  Warpinator
sumi@sumi-VirtualBox:~$ sudo setfattr -n user.mystream -v "Hello Worls!" myfile.txt
[sudo] password for sumi:
setfattr: myfile.txt: No such file or directory
sumi@sumi-VirtualBox:~$ touch myfile.txt
sumi@sumi-VirtualBox:~$ sudo setfattr -n user.mystream -v "Hello Worls!" myfile.txt
sumi@sumi-VirtualBox:~$ sudo getfattr -n user.mystream myfile.txt
# file: myfile.txt
user.mystream="Hello Worls!"
```

Now, add multimedia files like video and audio files into the datastream directory and we can view this with the help of **ls** command,

```
sumi@sumi-VirtualBox:~$ ls Datastream
fire.mp4  flowers.jpeg  road.jpeg  video.mp4
```

Open a terminal window and navigate to the directory containing the DataStream.

Run the following command to generate a report of all the files that Foremost can recover from the DataStream

Foremost -v -t all -i <Datastream>

In place of datastream, replace it with name and path of the Datastream file.

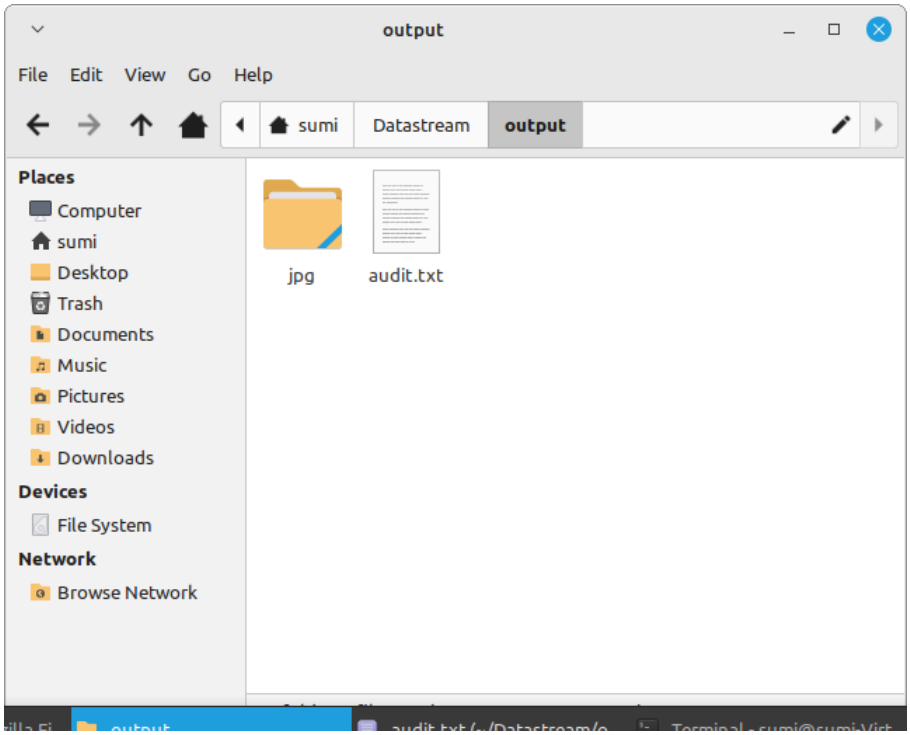
```
sumi@sumi-VirtualBox:~$ cd Datastream
sumi@sumi-VirtualBox:~/Datastream$ foremost -v -t all -i road.jpeg
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Apr  7 21:19:54 2023
Invocation: foremost -v -t all -i road.jpeg
Output directory: /home/sumi/Datastream/output
Configuration file: /etc/foremost.conf
Processing: road.jpeg
|------------------------------------------------------------------
File: road.jpeg
Start: Fri Apr  7 21:19:54 2023
Length: 12 KB (12494 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000000.jpg          12 KB               0
*|
Finish: Fri Apr  7 21:19:54 2023

1 FILES EXTRACTED

jpg:= 1
------------------------------------------------------------------

Foremost finished at Fri Apr  7 21:19:54 2023
```

The above example is for an image calledroad.jpeg, Once Foremost has generated a report, you can examine the output and identify the video files that have been recovered.

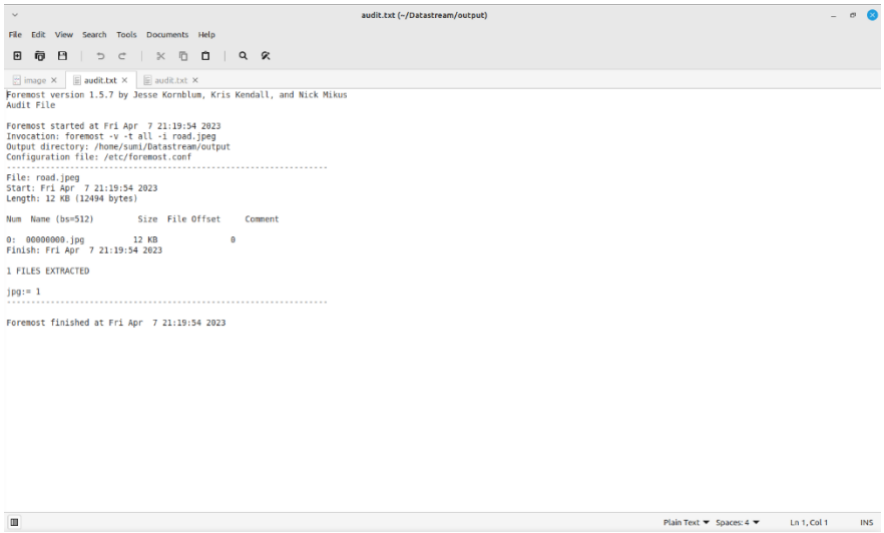
Foremost will typically recover files with names based on their file type, such as 00000123.avi for an AVI video file.

You can then view the recovered files to determine if they are partial or full multimedia files (video files) and extract any relevant evidence.

It created an file called output with jpg file and audit .txt in it



In audit.txt, you see this!



For video Files:

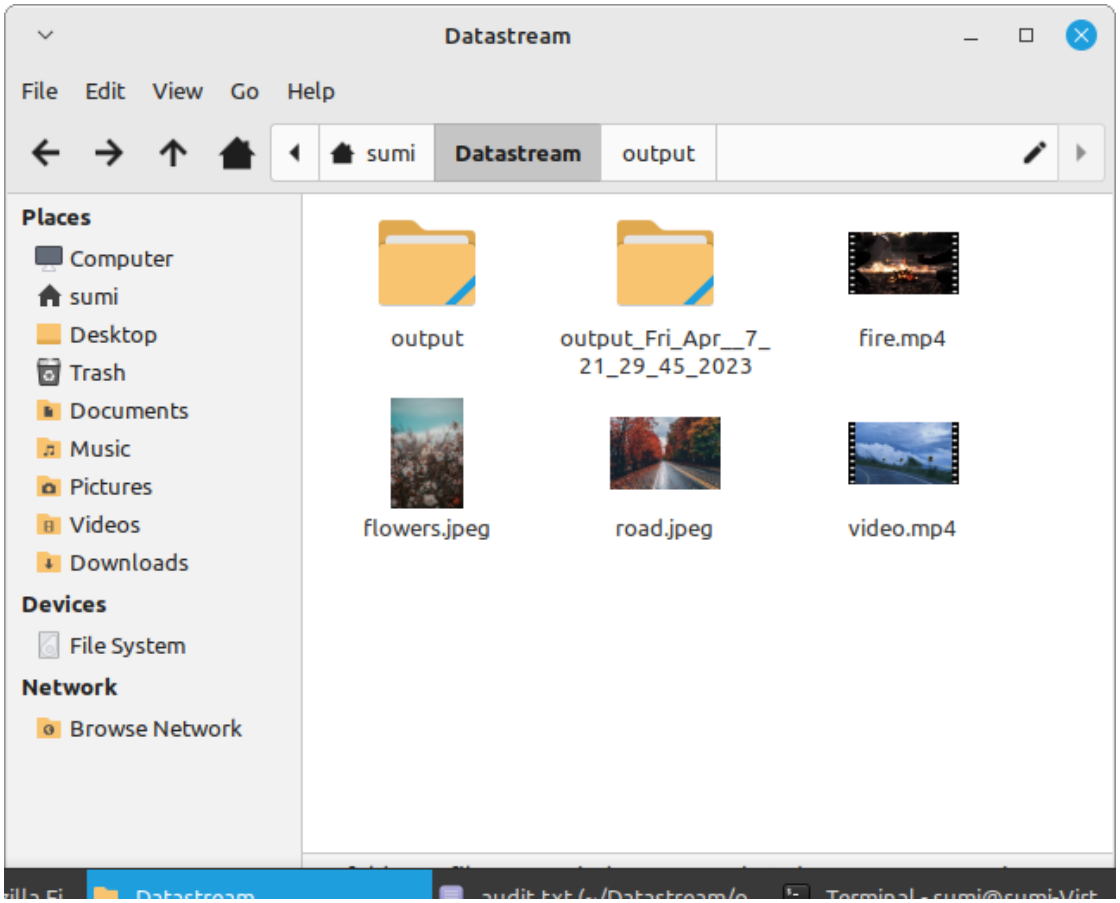
Same process for video files also,

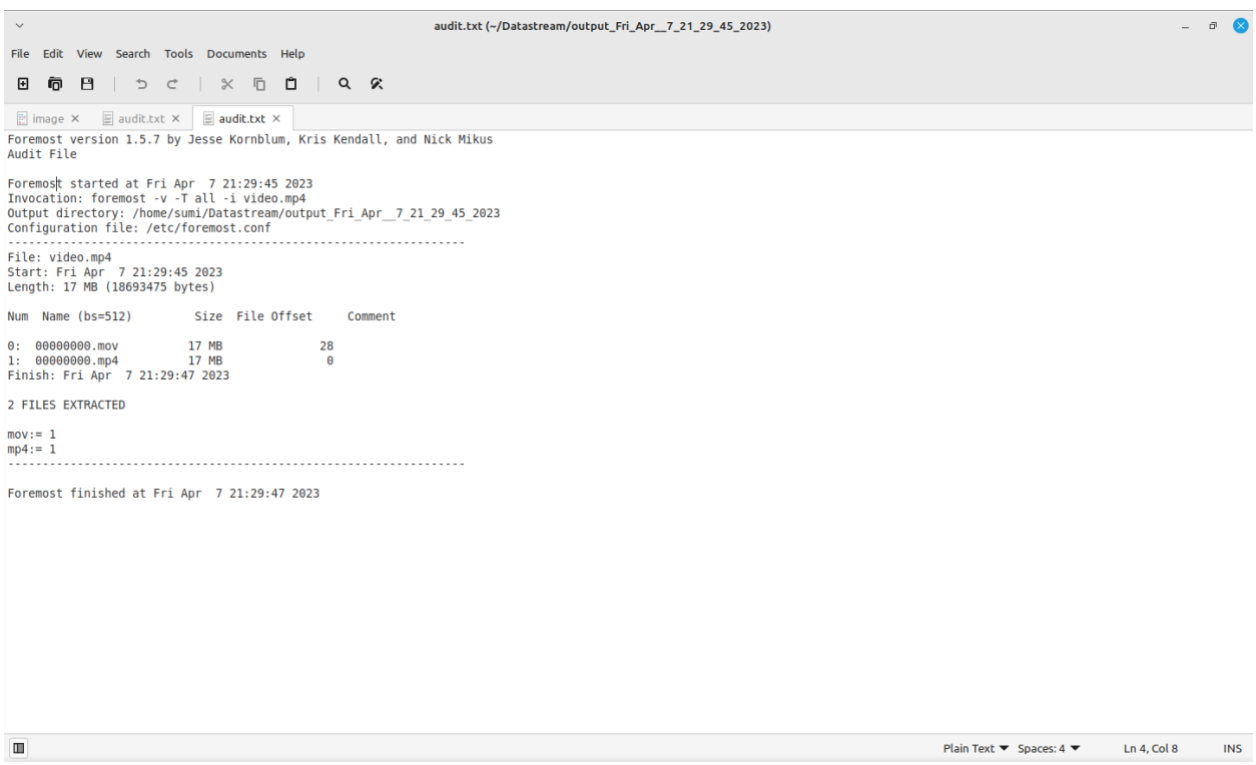
After adding them to our Datastream , we have to write the following command

Foremost -v -t all -i video.mp4

We get following output,

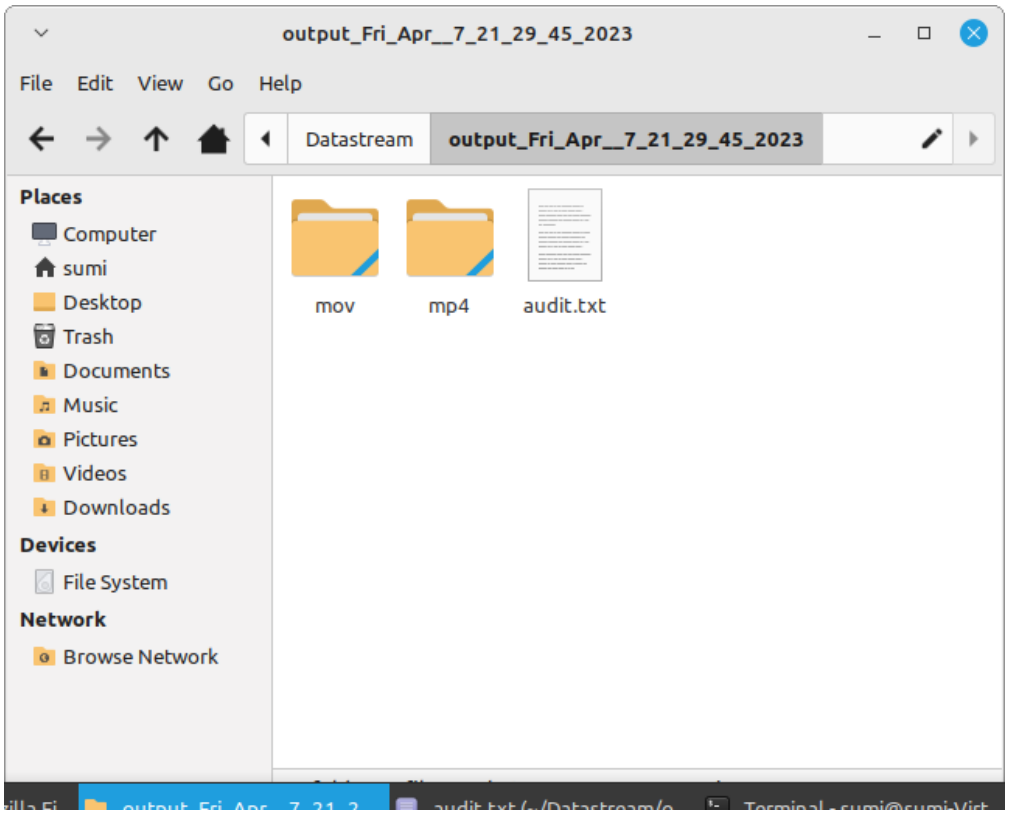
```
sumi@sumi-VirtualBox:~/Datastream$ foremost -v -T all -i
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall,
Audit File

Foremost started at Fri Apr  7 21:29:45 2023
Invocation: foremost -v -T all -i video.mp4
Output directory: /home/sumi/Datastream/output_Fri_Apr__
Configuration file: /etc/foremost.conf
Processing: video.mp4
|------------------------------------------------------
File: video.mp4
Start: Fri Apr  7 21:29:45 2023
Length: 17 MB (18693475 bytes)

Num      Name (bs=512)         Size      File Offset

0:      00000000.mov          17 MB              28
1:      00000000.mp4          17 MB               0
*|
Finish: Fri Apr  7 21:29:47 2023

2 FILES EXTRACTED

mov:= 1
mp4:= 1
------------------------------------------------------

Foremost finished at Fri Apr  7 21:29:47 2023
sumi@sumi-VirtualBox:~/Datastream$
```

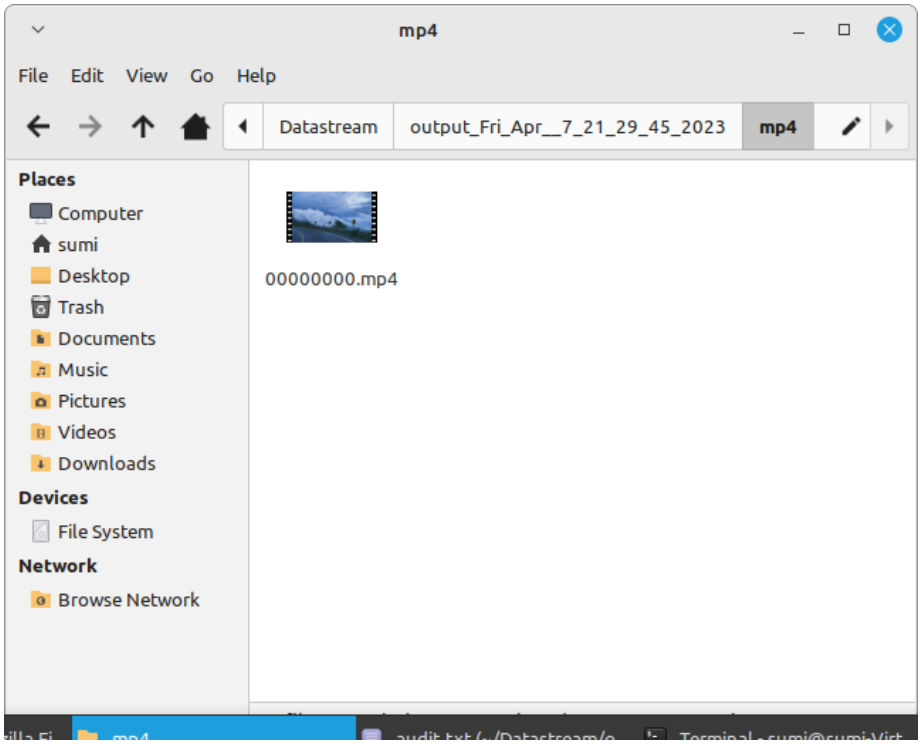

Datastream
File Edit View Go Help
sumi
Datastream
output
Places
Computer
sumi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
output
output_Fri_Apr__7_21_29_45_2023
fire.mp4
flowers.jpeg
road.jpeg
video.mp4


audit.txt (~/Datastream/output_Fri_Apr__7_21_29_45_2023)
File Edit View Search Tools Documents Help
image
audit.txt
audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Fri Apr 7 21:29:45 2023
Invocation: foremost -v -T all -i video.mp4
Output directory: /home/sumi/Datastream/output_Fri_Apr__7_21_29_45_2023
Configuration file: /etc/foremost.conf

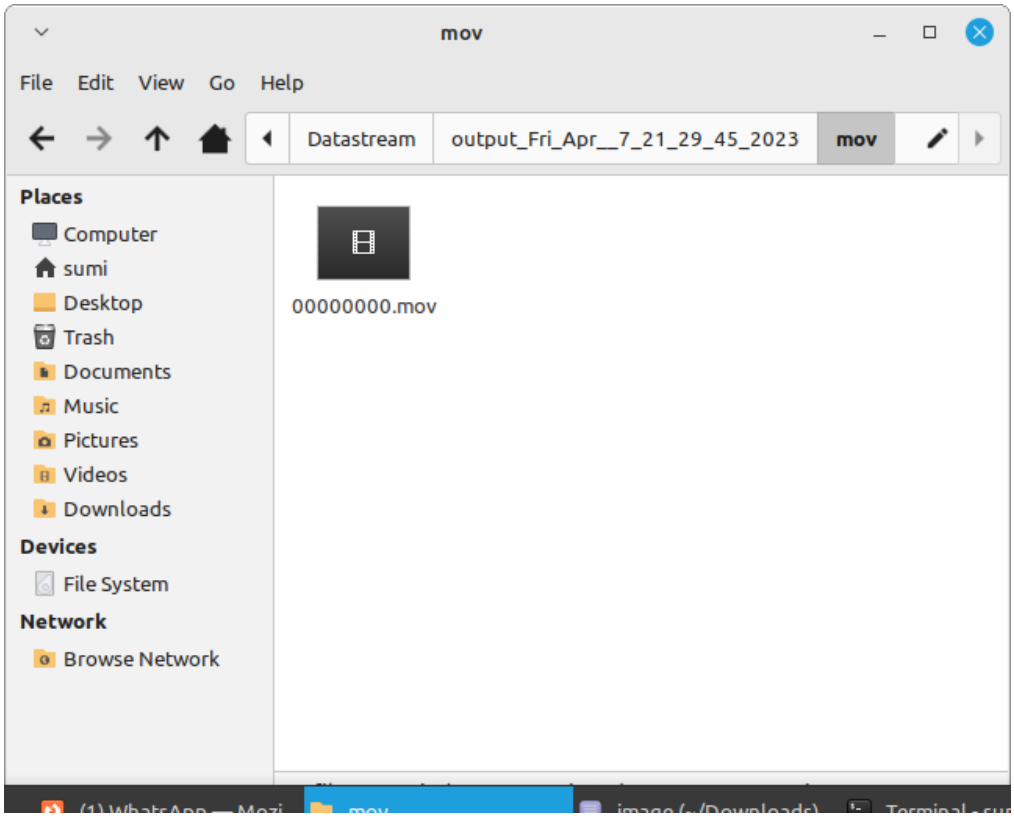
File: video.mp4
Start: Fri Apr 7 21:29:45 2023
Length: 17 MB (18693475 bytes)
Num Name (bs=512) Size File Offset Comment
0: 00000000.mov 17 MB 28
1: 00000000.mp4 17 MB 0
Finish: Fri Apr 7 21:29:47 2023
2 FILES EXTRACTED
mov:= 1
mp4:= 1

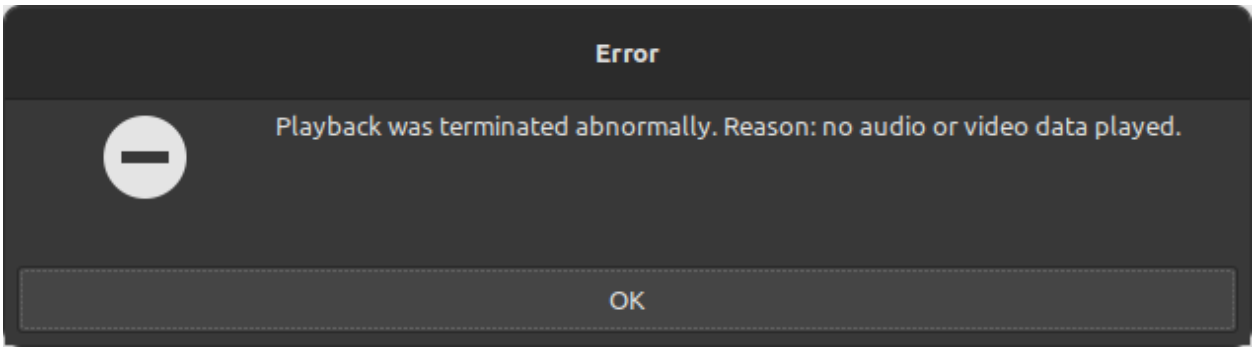
Foremost finished at Fri Apr 7 21:29:47 2023
Plain Text
Spaces: 4
Ln 4, Col 8
INS


output_Fri_Apr__7_21_29_45_2023
File Edit View Go Help
Datastream
output_Fri_Apr__7_21_29_45_2023
Places
Computer
sumi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
mov
mp4
audit.txt


mp4
File Edit View Go Help
Datastream
output_Fri_Apr__7_21_29_45_2023
mp4
Places
Computer
sumi
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
00000000.mp4

For partial file,





It is partial because, the file is not completely recovered, so this is less than actual size of the file and it is partial.

To determine whether a file is a full or partial multimedia file using Foremost, you should look at the size of the recovered file. If the file size is larger than expected for the type of file, it may be a partial file that has not been fully recovered. For example, if you recover an MP3 file that is only 1 MB in size, it is likely that this is a partial file that does not contain the full audio content.

Alternatively, you can also look at the file header to determine whether the file is a full or partial multimedia file. The header of a multimedia file contains information about the file format and can be used to determine whether the file is complete or not. If the header of the file is incomplete or corrupted, it is likely that the file is a partial multimedia file.

So, with the help of the report and information obtained from foremost, we can etermine whether a file is full or partial multimedia file!

My GitHub link:

https://github.com/sumeetha123/INT301_CA3