Tên: Trần Minh Triết

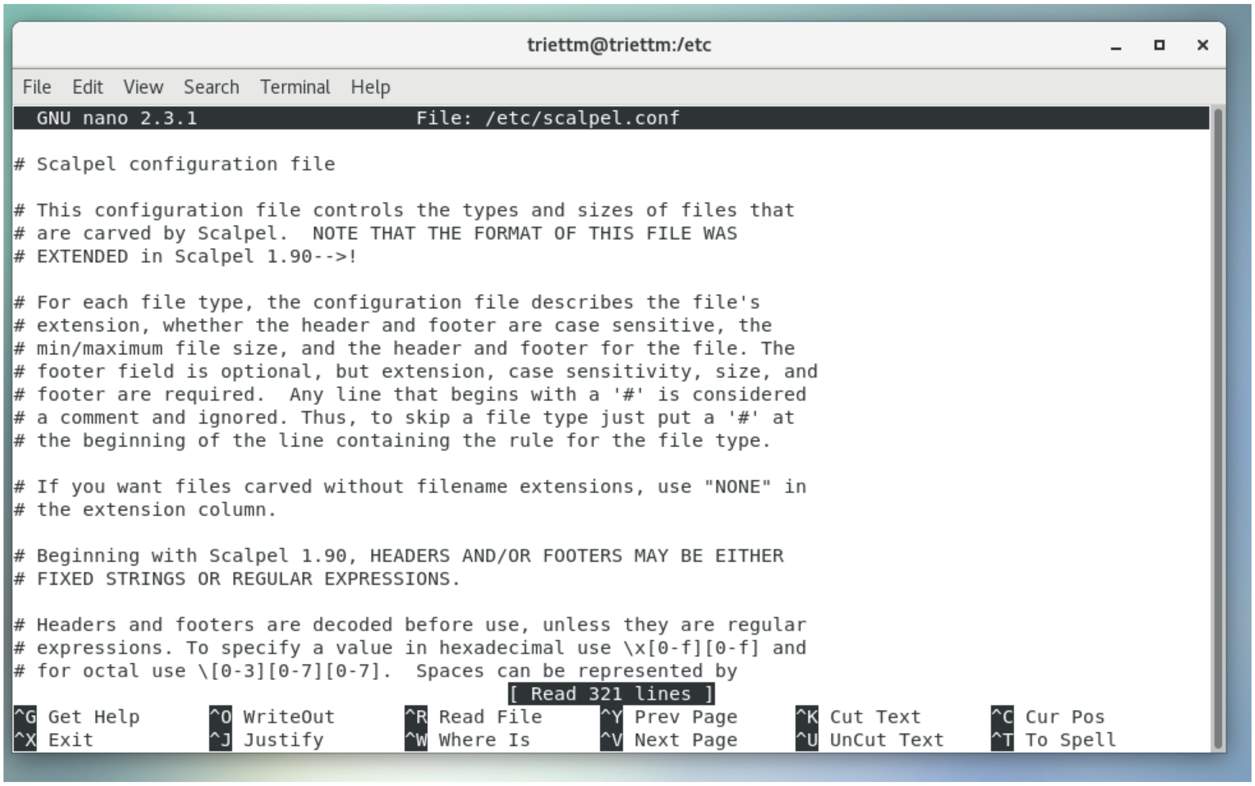
MSSV: SE172241

LAB 6

Recovering lost or deleted files with Scalpel

You will need the EPEL repository to complete this process (which is discussed in a previous chapter), but when you are ready, simply update the following configuration file to determine what types of files you would like to search for:

nano /etc/scalpel.conf



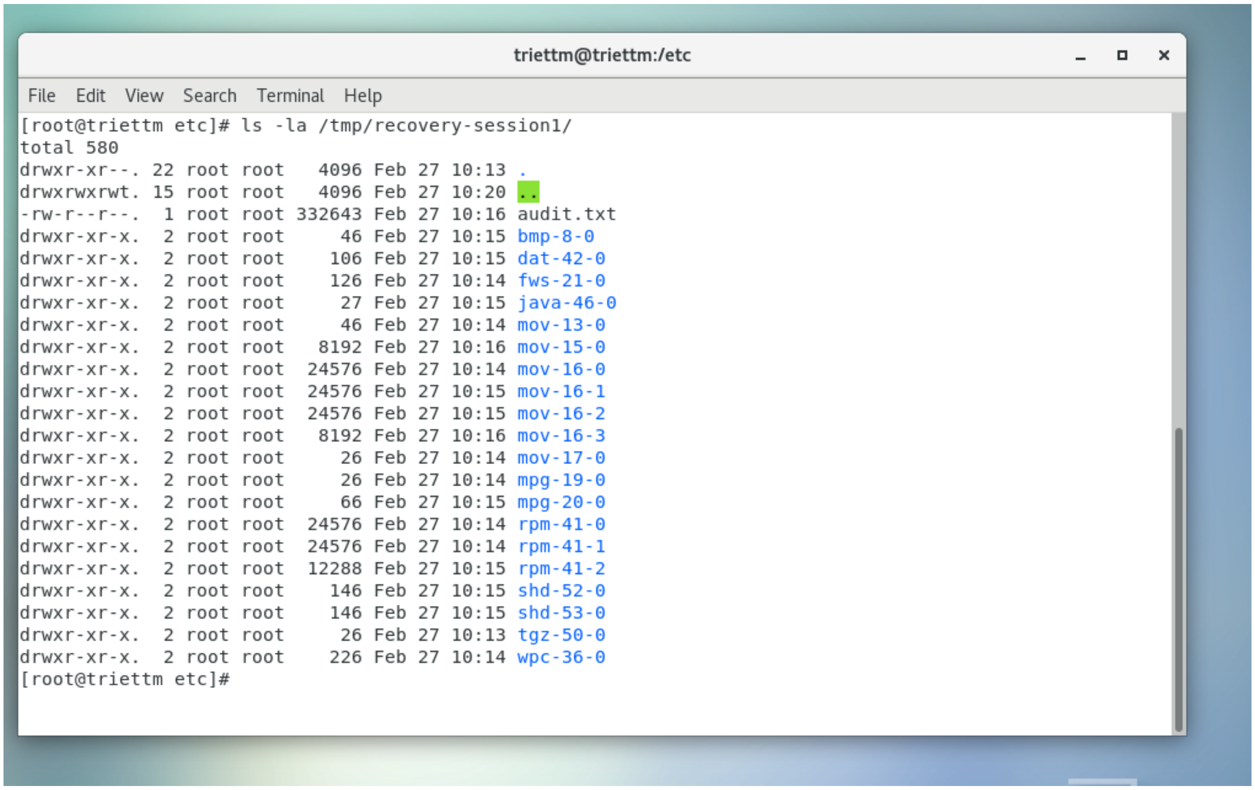
```
  GNU nano 2.3.1               File: /etc/scalpel.conf

# Scalpel configuration file

# This configuration file controls the types and sizes of files that
# are carved by Scalpel.  NOTE THAT THE FORMAT OF THIS FILE WAS
# EXTENDED in Scalpel 1.90-->!

# For each file type, the configuration file describes the file's
# extension, whether the header and footer are case sensitive, the
# min/maximum file size, and the header and footer for the file. The
# footer field is optional, but extension, case sensitivity, size, and
# footer are required.  Any line that begins with a '#' is considered
# a comment and ignored. Thus, to skip a file type just put a '#' at
# the beginning of the line containing the rule for the file type.

# If you want files carved without filename extensions, use "NONE" in
# the extension column.

# Beginning with Scalpel 1.90, HEADERS AND/OR FOOTERS MAY BE EITHER
# FIXED STRINGS OR REGULAR EXPRESSIONS.

# Headers and footers are decoded before use, unless they are regular
# expressions. To specify a value in hexadecimal use \x[0-f][0-f] and
# for octal use \[0-3][0-7][0-7].  Spaces can be represented by
                                            [ Read 321 lines ]
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

scalpel /dev/sda1 -o /tmp/recovery-session1

Using the above command, we start using scalpel to recovery data from the disk sda1 to /tmp/recovery-session1

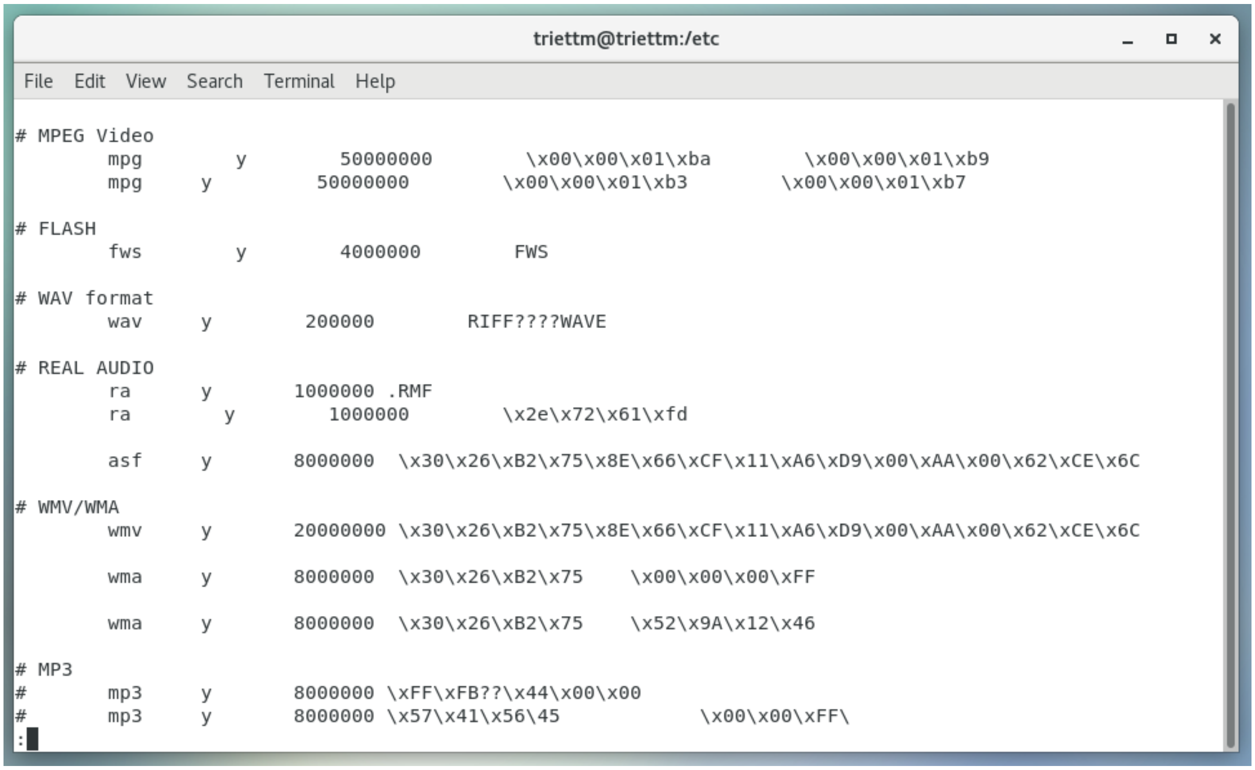
As we do not specify any file type, Scalpel will extract all file types and deleted files to the destination location.

Testing by listing the folder contents



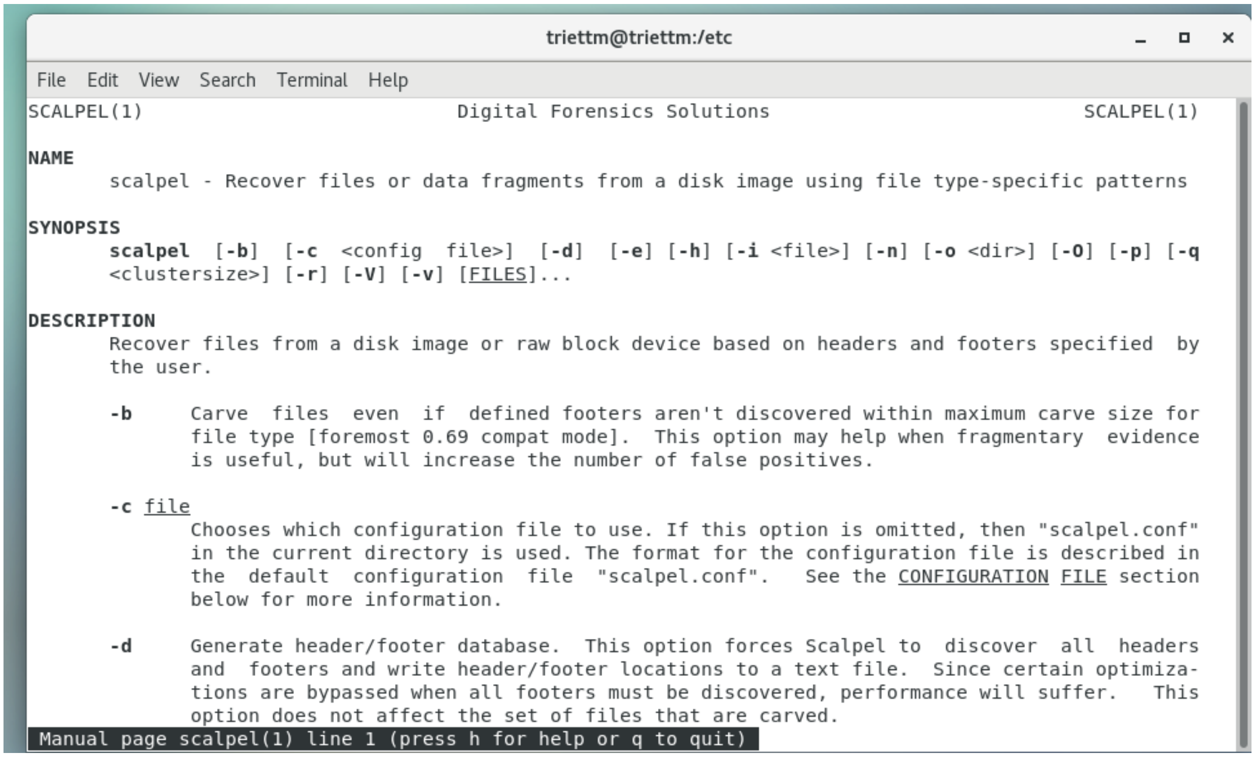
```
[root@triettm etc]# ls -la /tmp/recovery-session1/
total 580
drwxr-xr--. 22 root root   4096 Feb 27 10:13 .
drwxrwxrwt. 15 root root   4096 Feb 27 10:20 ..
-rw-r--r--.  1 root root 332643 Feb 27 10:16 audit.txt
drwxr-xr-x.  2 root root     46 Feb 27 10:15 bmp-8-0
drwxr-xr-x.  2 root root    106 Feb 27 10:15 dat-42-0
drwxr-xr-x.  2 root root    126 Feb 27 10:14 fws-21-0
drwxr-xr-x.  2 root root     27 Feb 27 10:15 java-46-0
drwxr-xr-x.  2 root root     46 Feb 27 10:14 mov-13-0
drwxr-xr-x.  2 root root   8192 Feb 27 10:16 mov-15-0
drwxr-xr-x.  2 root root  24576 Feb 27 10:14 mov-16-0
drwxr-xr-x.  2 root root  24576 Feb 27 10:15 mov-16-1
drwxr-xr-x.  2 root root  24576 Feb 27 10:15 mov-16-2
drwxr-xr-x.  2 root root   8192 Feb 27 10:16 mov-16-3
drwxr-xr-x.  2 root root     26 Feb 27 10:14 mov-17-0
drwxr-xr-x.  2 root root     26 Feb 27 10:14 mpg-19-0
drwxr-xr-x.  2 root root     66 Feb 27 10:15 mpg-20-0
drwxr-xr-x.  2 root root  24576 Feb 27 10:14 rpm-41-0
drwxr-xr-x.  2 root root  24576 Feb 27 10:14 rpm-41-1
drwxr-xr-x.  2 root root  12288 Feb 27 10:15 rpm-41-2
drwxr-xr-x.  2 root root    146 Feb 27 10:15 shd-52-0
drwxr-xr-x.  2 root root    146 Feb 27 10:15 shd-53-0
drwxr-xr-x.  2 root root     26 Feb 27 10:13 tgz-50-0
drwxr-xr-x.  2 root root    226 Feb 27 10:14 wpc-36-0
[root@triettm etc]#
```

less /tmp/recovery-session1/audit.txt



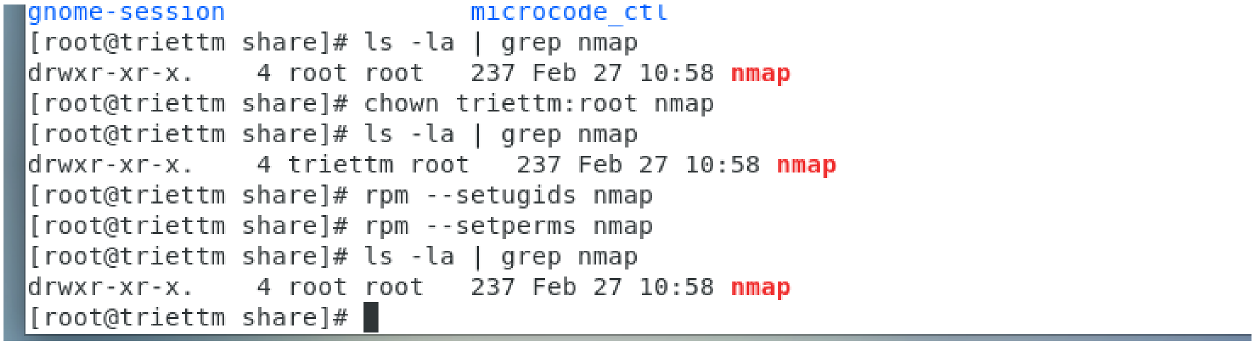
```

# MPEG Video
        mpg        y        50000000        \x00\x00\x01\xba        \x00\x00\x01\xb9
        mpg     y        50000000        \x00\x00\x01\xb3        \x00\x00\x01\xb7

# FLASH
        fws        y        4000000        FWS

# WAV format
        wav     y        200000        RIFF????WAVE

# REAL AUDIO
        ra      y       1000000 .RMF
        ra        y        1000000        \x2e\x72\x61\xfd

        asf     y       8000000  \x30\x26\xB2\x75\x8E\x66\xCF\x11\xA6\xD9\x00\xAA\x00\x62\xCE\x6C

# WMV/WMA
        wmv     y       20000000 \x30\x26\xB2\x75\x8E\x66\xCF\x11\xA6\xD9\x00\xAA\x00\x62\xCE\x6C

        wma     y       8000000  \x30\x26\xB2\x75    \x00\x00\x00\xFF

        wma     y       8000000  \x30\x26\xB2\x75    \x52\x9A\x12\x46

# MP3
#       mp3     y       8000000 \xFF\xFB??\x44\x00\x00
#       mp3     y       8000000 \x57\x41\x56\45           \x00\x00\xFF\
:
```

man scalpel



```
SCALPEL(1)                    Digital Forensics Solutions                   SCALPEL(1)

NAME
       scalpel - Recover files or data fragments from a disk image using file type-specific patterns

SYNOPSIS
       scalpel  [-b]  [-c  <config  file>]  [-d]  [-e] [-h] [-i <file>] [-n] [-o <dir>] [-O] [-p] [-q
       <clustersize>] [-r] [-V] [-v] [FILES]...

DESCRIPTION
       Recover files from a disk image or raw block device based on headers and footers specified  by
       the user.

       -b     Carve  files  even  if  defined footers aren't discovered within maximum carve size for
              file type [foremost 0.69 compat mode].  This option may help when fragmentary  evidence
              is useful, but will increase the number of false positives.

       -c file
              Chooses which configuration file to use. If this option is omitted, then "scalpel.conf"
              in the current directory is used. The format for the configuration file is described in
              the  default  configuration  file  "scalpel.conf".   See the CONFIGURATION FILE section
              below for more information.

       -d     Generate header/footer database.  This option forces Scalpel to  discover  all  headers
              and  footers and write header/footer locations to a text file.  Since certain optimiza-
              tions are bypassed when all footers must be discovered, performance will suffer.   This
              option does not affect the set of files that are carved.
 Manual page scalpel(1) line 1 (press h for help or q to quit)
```

Restoring file and directory permissions



```
gnome-session                 microcode_ctl
[root@triettm share]# ls -la | grep nmap
drwxr-xr-x.    4 root root   237 Feb 27 10:58 nmap
[root@triettm share]# chown triettm:root nmap
[root@triettm share]# ls -la | grep nmap
drwxr-xr-x.    4 triettm root   237 Feb 27 10:58 nmap
[root@triettm share]# rpm --setugids nmap
[root@triettm share]# rpm --setperms nmap
[root@triettm share]# ls -la | grep nmap
drwxr-xr-x.    4 root root   237 Feb 27 10:58 nmap
[root@triettm share]# 
```

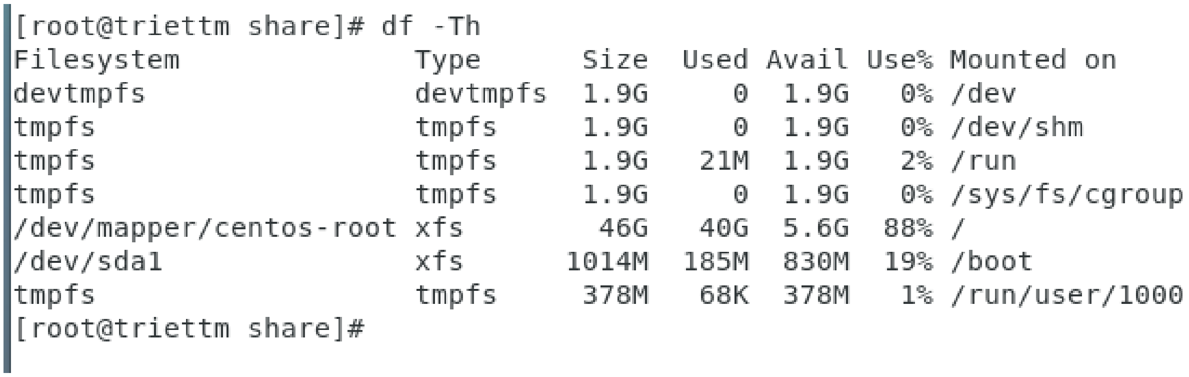
At first I install tool nmap with rpm command:

rpm -vhU https://nmap.org/dist/nmap-7.93-1.x86_64.rpm

Then as the above image, you can see that the owner of the package is root, group is root.

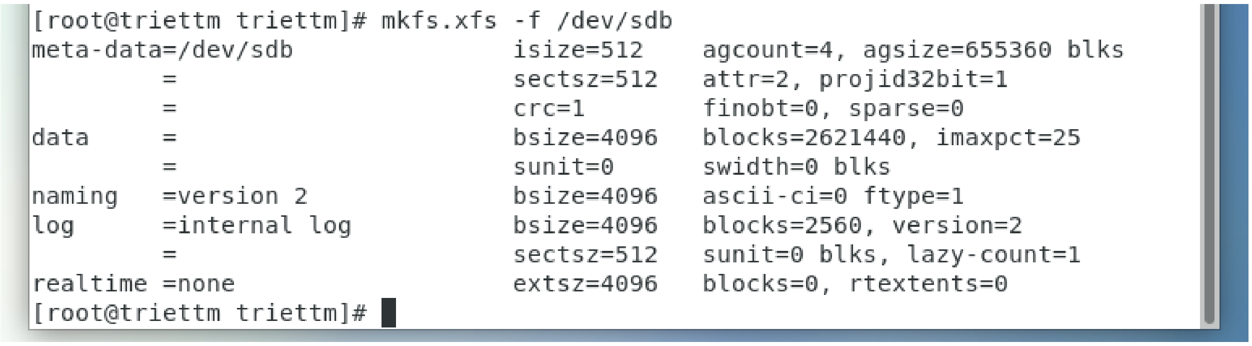
Then I change the owner of the packet and testing restore its permissions back to root again.

Working with and extending the XFS filesystem



```
[root@triettm share]# df -Th
Filesystem              Type      Size  Used Avail Use% Mounted on
devtmpfs                devtmpfs  1.9G     0  1.9G   0% /dev
tmpfs                   tmpfs     1.9G     0  1.9G   0% /dev/shm
tmpfs                   tmpfs     1.9G   21M  1.9G   2% /run
tmpfs                   tmpfs     1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/mapper/centos-root xfs        46G   40G  5.6G  88% /
/dev/sda1               xfs      1014M  185M  830M  19% /boot
tmpfs                   tmpfs     378M   68K  378M   1% /run/user/1000
[root@triettm share]#
```

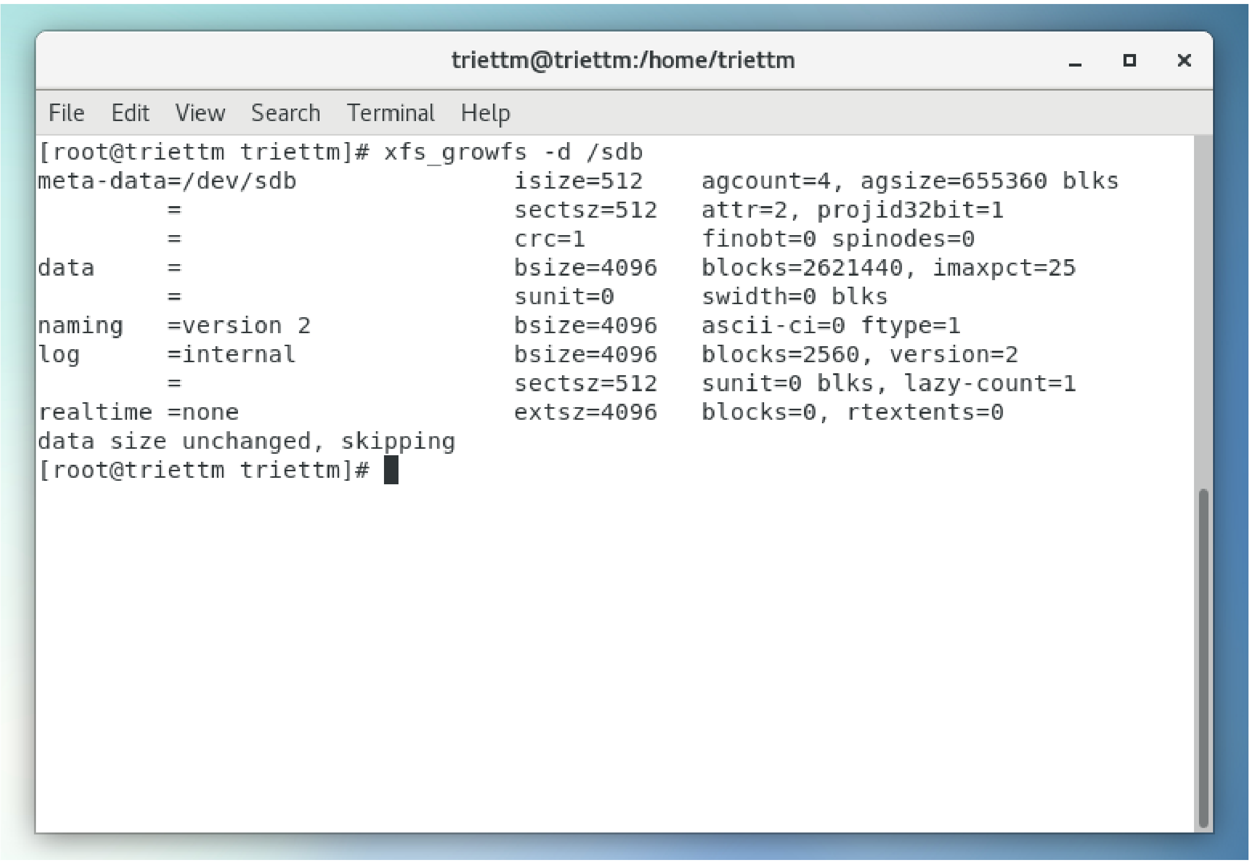
Cấu hình XFS cho ổ cứng



```
[root@triettm triettm]# mkfs.xfs -f /dev/sdb
meta-data=/dev/sdb               isize=512    agcount=4, agsize=655360 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=2621440, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
[root@triettm triettm]# 
```

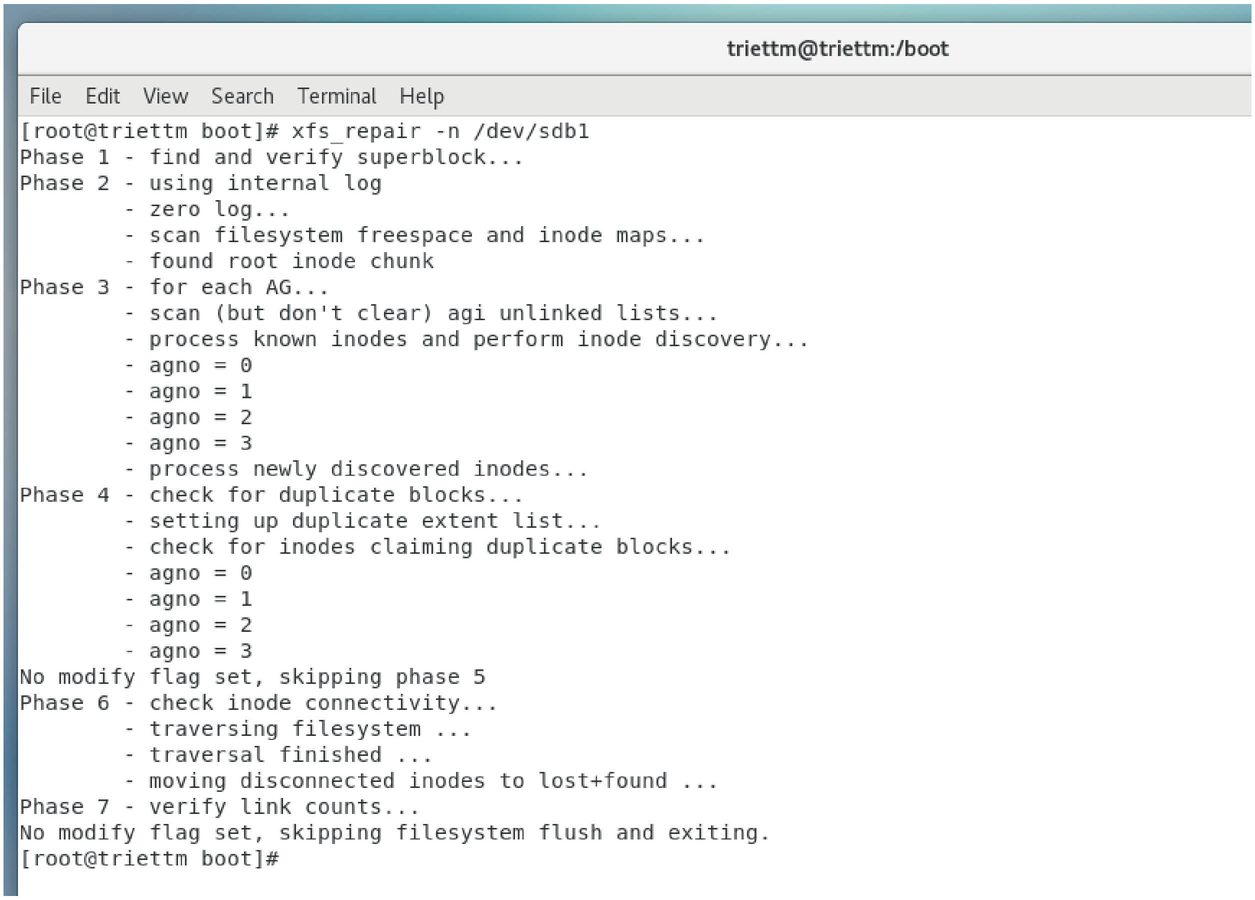
We have successfully config and mount the sdb hard disk with XFS file system.

In this respect, and as we will now see, XFS should be treated in a different way to a comparable ext3- or ext4-based system. However, if you need to extend the filesystem, then you will be happy to know that XFS comes complete with a standard tool known as `xfs_growfs` that can be used in the following way:

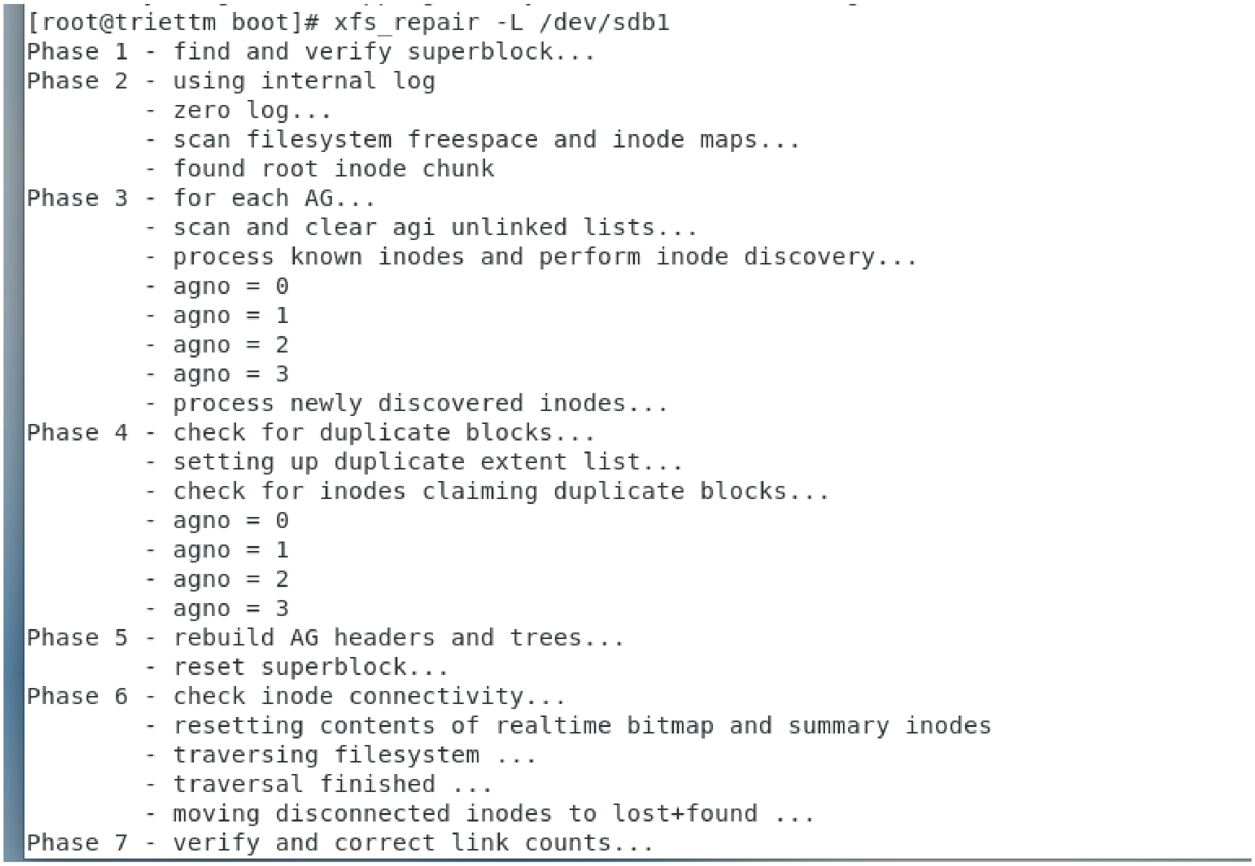

triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
[root@triettm triettm]# xfs_growfs -d /sdb
meta-data=/dev/sdb               isize=512    agcount=4, agsize=655360 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0 spinodes=0
data     =                       bsize=4096   blocks=2621440, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal               bsize=4096   blocks=2560, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data size unchanged, skipping
[root@triettm triettm]# 
```

Running repairs on XFS

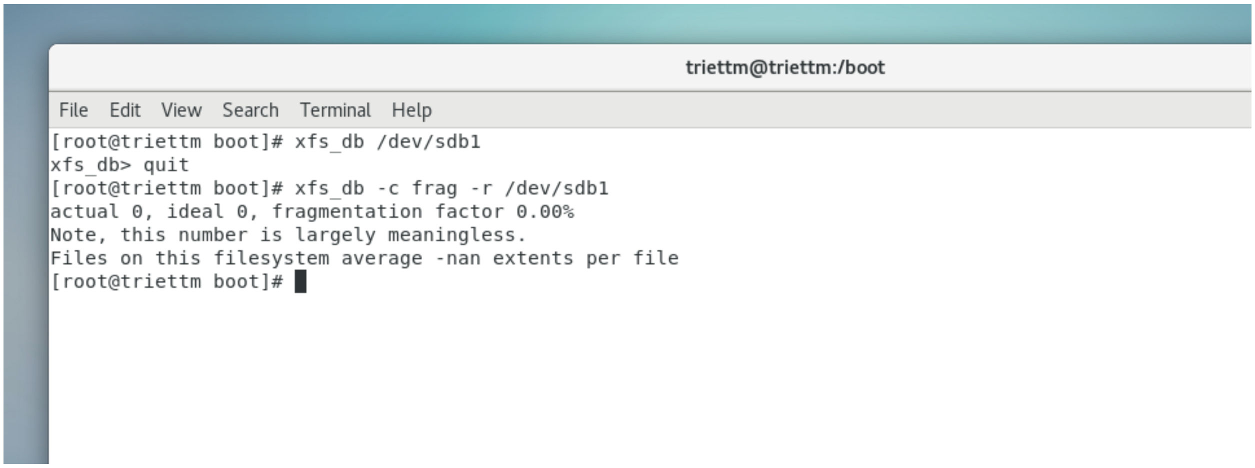


```
[root@triettm boot]# xfs_repair -n /dev/sdb1
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan (but don't clear) agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
No modify flag set, skipping phase 5
Phase 6 - check inode connectivity...
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify link counts...
No modify flag set, skipping filesystem flush and exiting.
[root@triettm boot]#
```



```
[root@triettm boot]# xfs_repair -L /dev/sdb1
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
```

Investigating fragmentation on XFS

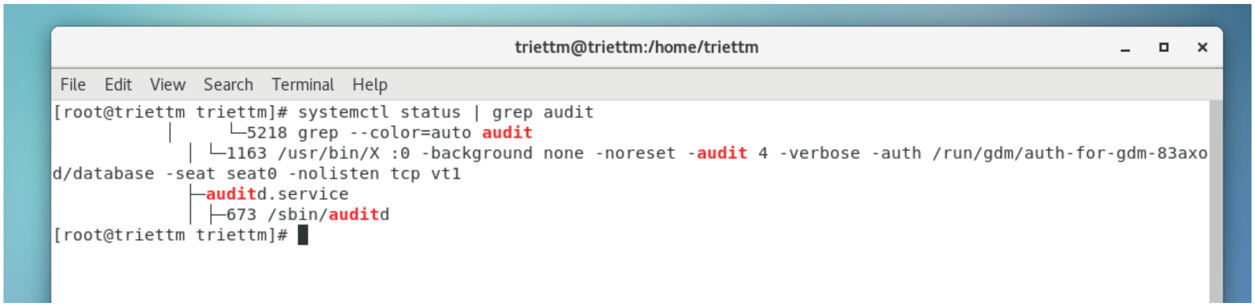


```
[root@triettm boot]# xfs_db /dev/sdb1
xfs_db> quit
[root@triettm boot]# xfs_db -c frag -r /dev/sdb1
actual 0, ideal 0, fragmentation factor 0.00%
Note, this number is largely meaningless.
Files on this filesystem average -nan extents per file
[root@triettm boot]# 
```

Auditing directories and files

An important task related to troubleshooting can arise from an understanding of activities commonly associated with the action of reading and writing files. CentOS 7 provides a simple utility for this. Known as `auditd`, this service (or daemon) starts during the boot process. Events are recorded to an associated log file found at `/var/log/audit` and as it runs in the background, you can check the current service status with:

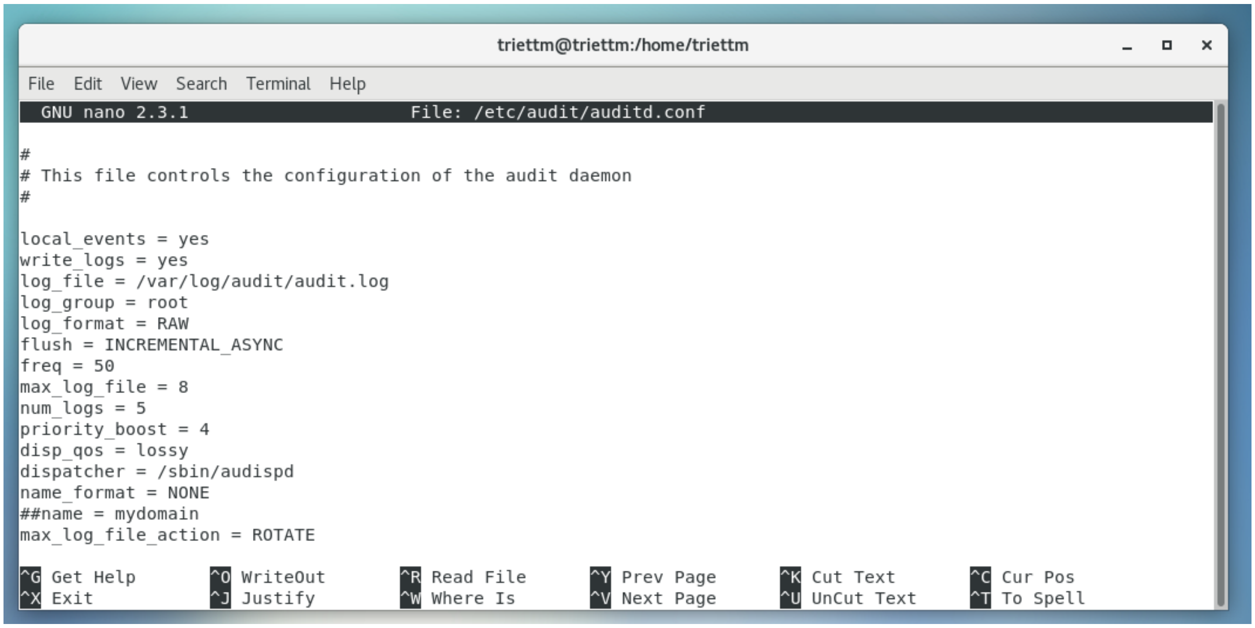
`systemctl status | grep audit`


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
[root@triettm triettm]# systemctl status | grep audit
           │     └─5218 grep --color=auto audit
             │ └─1163 /usr/bin/X :0 -background none -noreset -audit 4 -verbose -auth /run/gdm/auth-for-gdm-83axo
d/database -seat seat0 -nolisten tcp vt1
             ├─auditd.service
             │ ├─673 /sbin/auditd
[root@triettm triettm]# 
```

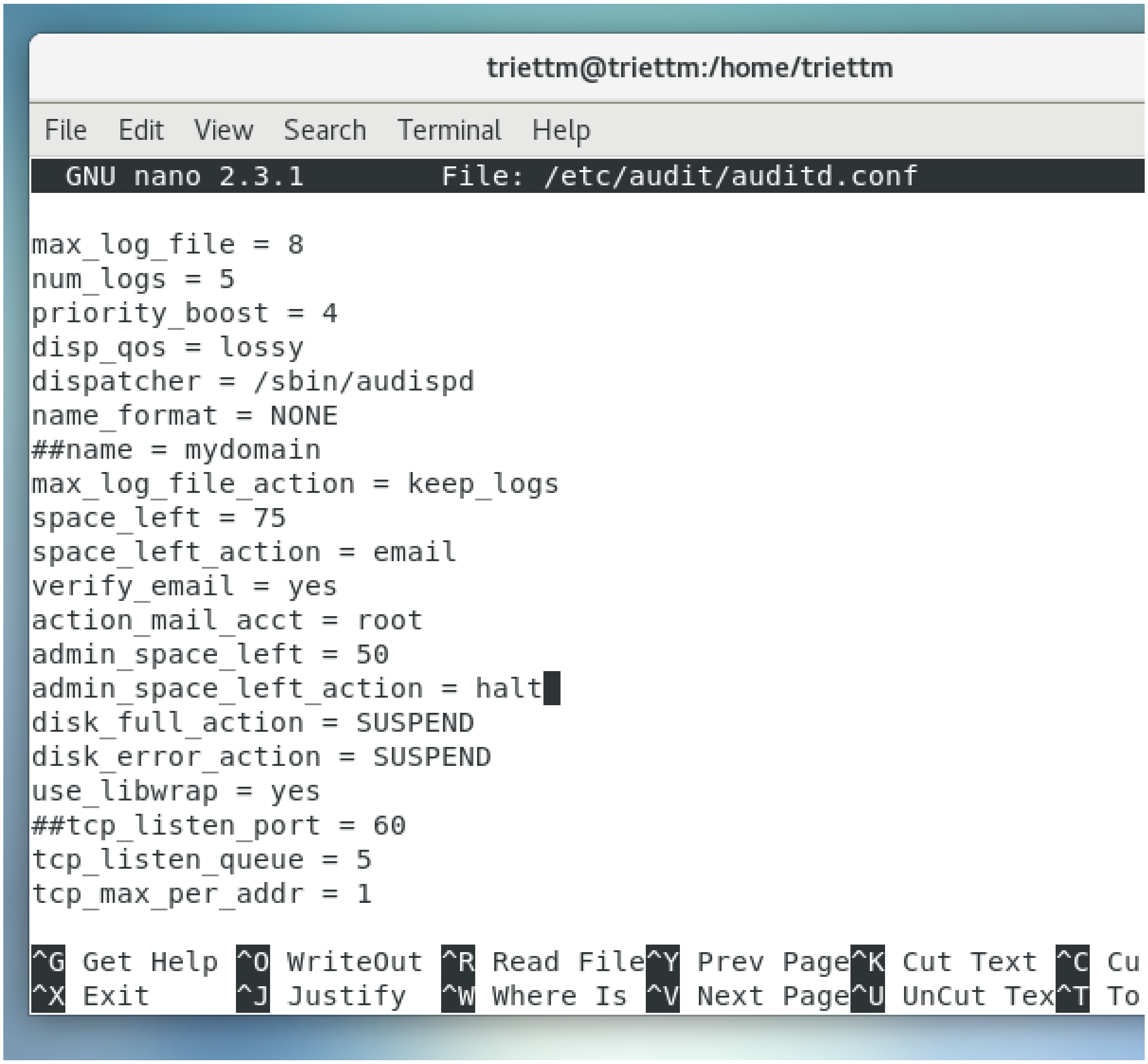
As we can see that the daemon auditd is running in the background.

It is possible to customize the auditing service and you can have direct access to manage the log file size, location, and associated attributes by accessing the following file with your favorite text editor:


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
  GNU nano 2.3.1                    File: /etc/audit/auditd.conf

#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE

^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

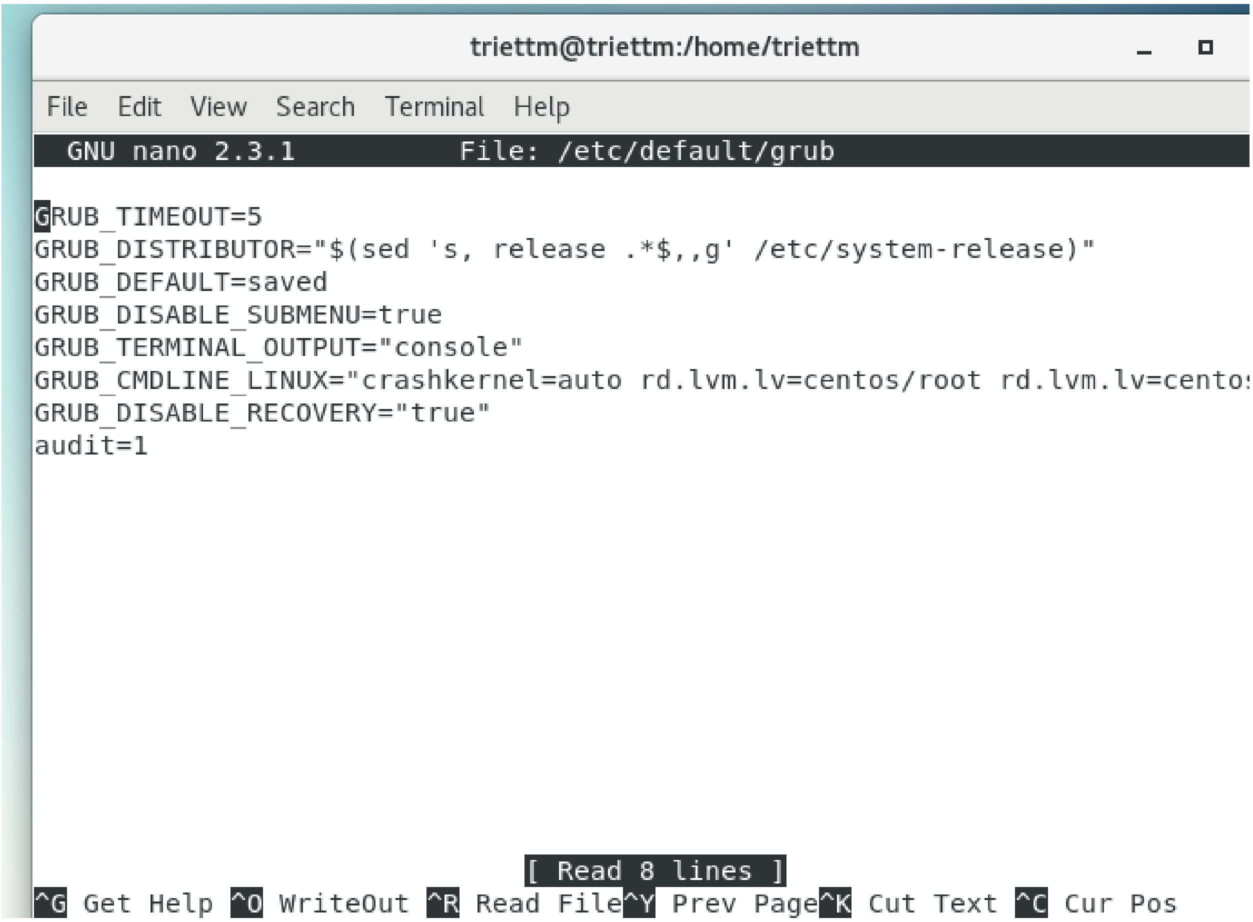
We can change the content of this file to change the behaviour of the auditd daemon.


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
  GNU nano 2.3.1         File: /etc/audit/auditd.conf

max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = keep_logs
space_left = 75
space_left_action = email
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = halt
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1

^G Get Help ^O WriteOut ^R Read File^Y Prev Page^K Cut Text ^C Cu
^X Exit     ^J Justify  ^W Where Is ^V Next Page^U UnCut Tex^T To
```

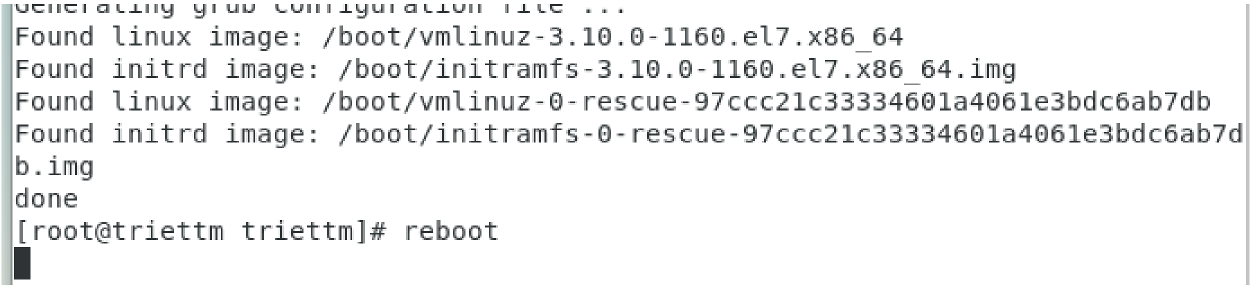
This action is severe and it is not something to jump into without doing your homework, but it will serve to remove the default action of rotating log files and replace it with an instruction to e-mail the root user.

Finally I open the /etc/default/grub to take advantage of the audit service flag for every process.



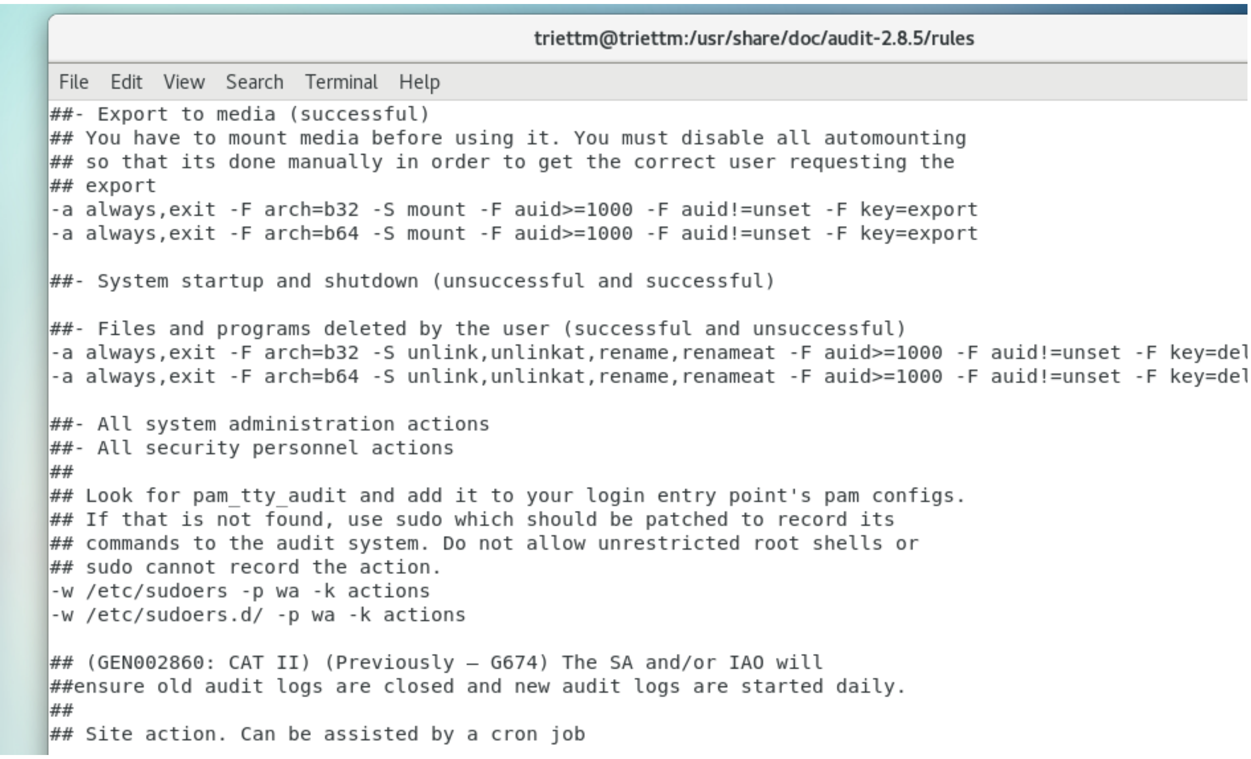
```
  GNU nano 2.3.1          File: /etc/default/grub

GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos
GRUB_DISABLE_RECOVERY="true"
audit=1

                              [ Read 8 lines ]
^G Get Help ^O WriteOut ^R Read File^Y Prev Page^K Cut Text ^C Cur Pos
```

Remember to regenerate grub with the following command and reboot

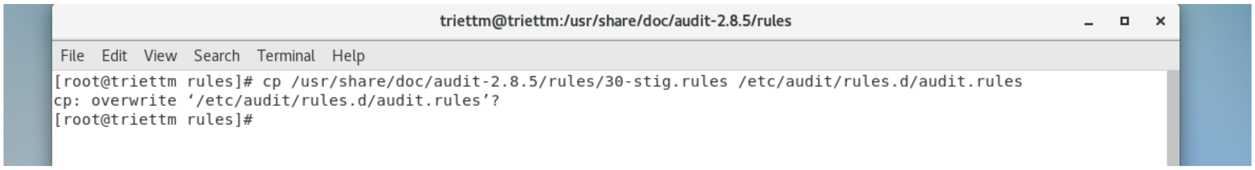


```
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-1160.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-1160.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-97ccc21c33334601a4061e3bdc6ab7db
Found initrd image: /boot/initramfs-0-rescue-97ccc21c33334601a4061e3bdc6ab7d
b.img
done
[root@triettm triettm]# reboot
```

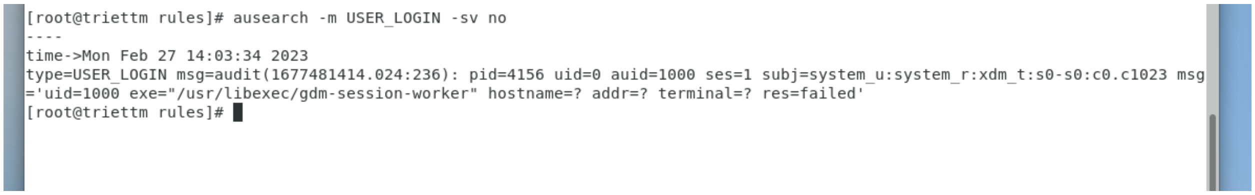
In my computer, the stig.rule file store inside this path /usr/share/doc/audit-2.8.5/rules/30-stig.rules


triettm@triettm:/usr/share/doc/audit-2.8.5/rules
File Edit View Search Terminal Help

```
##- Export to media (successful)
## You have to mount media before using it. You must disable all automounting
## so that its done manually in order to get the correct user requesting the
## export
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -F key=export
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -F key=export

##- System startup and shutdown (unsuccessful and successful)

##- Files and programs deleted by the user (successful and unsuccessful)
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F auid>=1000 -F auid!=unset -F key=del
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F auid>=1000 -F auid!=unset -F key=del

##- All system administration actions
##- All security personnel actions
##
## Look for pam_tty_audit and add it to your login entry point's pam configs.
## If that is not found, use sudo which should be patched to record its
## commands to the audit system. Do not allow unrestricted root shells or
## sudo cannot record the action.
-w /etc/sudoers -p wa -k actions
-w /etc/sudoers.d/ -p wa -k actions

## (GEN002860: CAT II) (Previously – G674) The SA and/or IAO will
##ensure old audit logs are closed and new audit logs are started daily.
##
## Site action. Can be assisted by a cron job
```


triettm@triettm:/usr/share/doc/audit-2.8.5/rules
File Edit View Search Terminal Help

```
[root@triettm rules]# cp /usr/share/doc/audit-2.8.5/rules/30-stig.rules /etc/audit/rules.d/audit.rules
cp: overwrite ‘/etc/audit/rules.d/audit.rules’?
[root@triettm rules]#
```

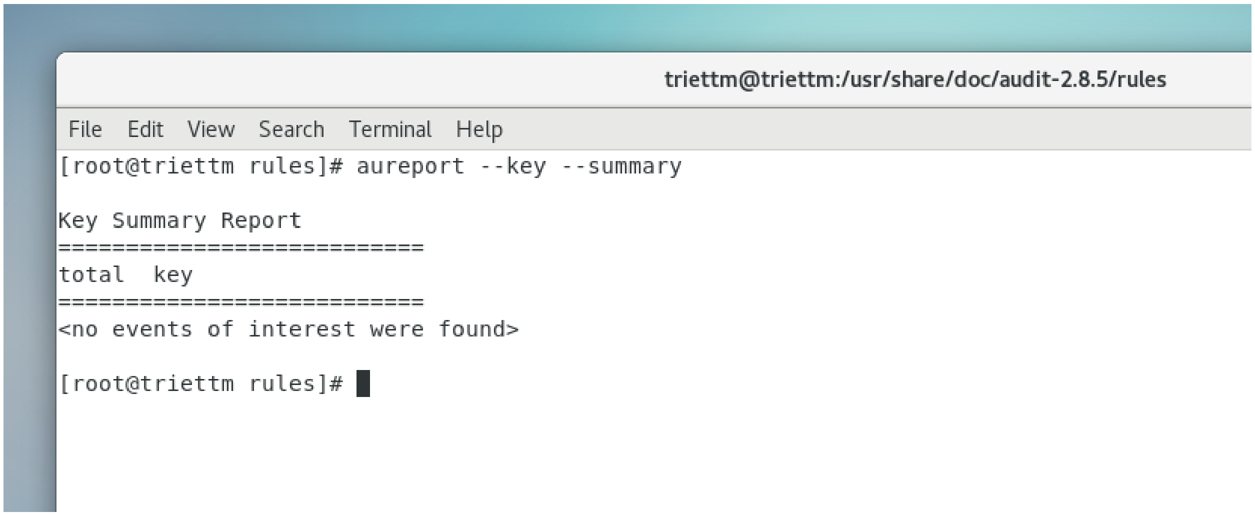


```
[root@triettm rules]# ausearch -m USER_LOGIN -sv no
----
time->Mon Feb 27 14:03:34 2023
type=USER_LOGIN msg=audit(1677481414.024:236): pid=4156 uid=0 auid=1000 ses=1 subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg
='uid=1000 exe="/usr/libexec/gdm-session-worker" hostname=? addr=? terminal=? res=failed'
[root@triettm rules]# █
```

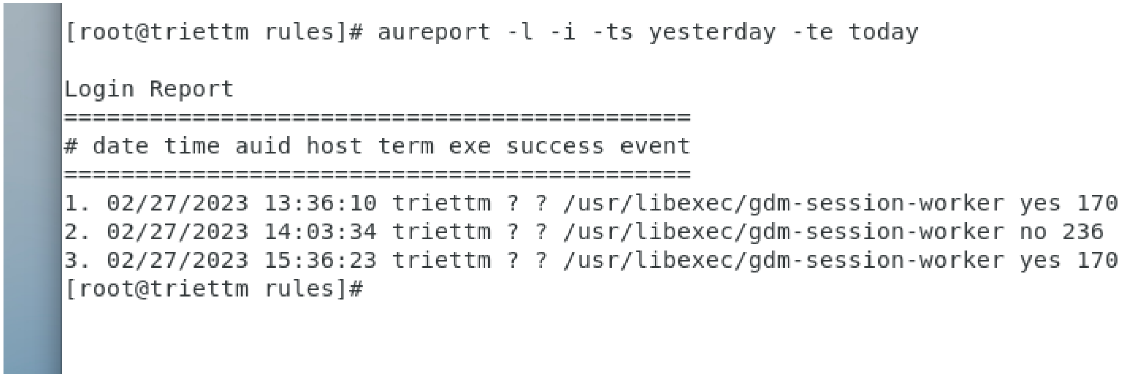
As an alternative to this, you can use `aureport` to produce a series of audits in the following way:

To monitor unusual behavior, you can use:

aureport --key –summary


triettm@triettm:/usr/share/doc/audit-2.8.5/rules
File Edit View Search Terminal Help

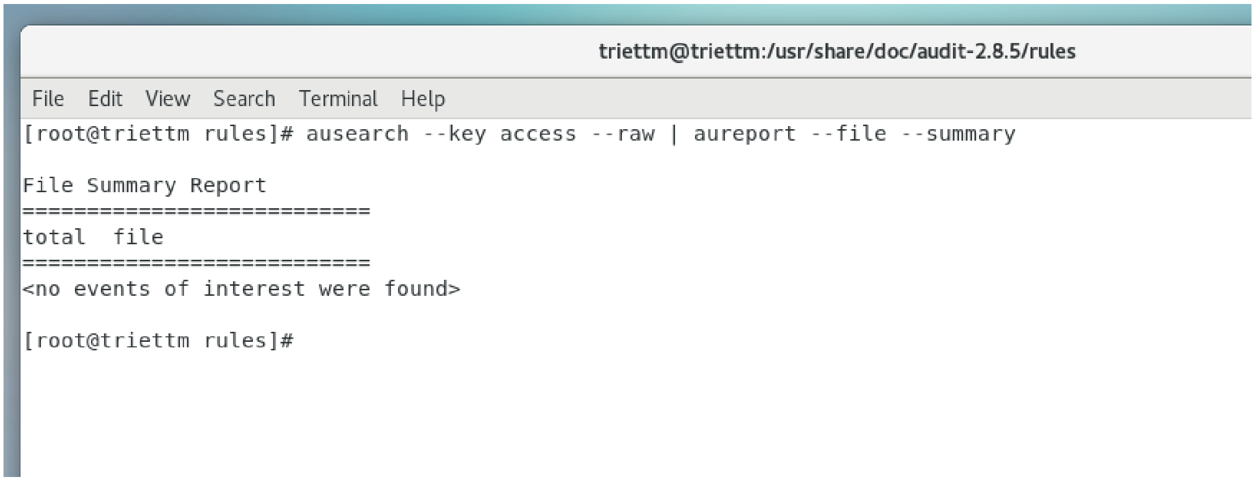
```
[root@triettm rules]# aureport --key --summary

Key Summary Report
===========================
total  key
===========================
<no events of interest were found>

[root@triettm rules]# 
```



```
[root@triettm rules]# aureport -l -i -ts yesterday -te today

Login Report
============================================
# date time auid host term exe success event
============================================
1. 02/27/2023 13:36:10 triettm ? ? /usr/libexec/gdm-session-worker yes 170
2. 02/27/2023 14:03:34 triettm ? ? /usr/libexec/gdm-session-worker no 236
3. 02/27/2023 15:36:23 triettm ? ? /usr/libexec/gdm-session-worker yes 170
[root@triettm rules]#
```

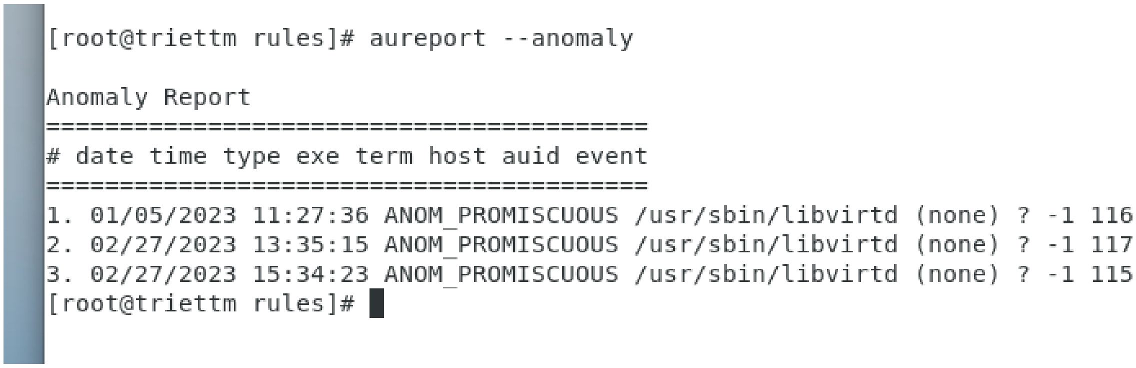
To review access violations, you can try:

ausearch --key access --raw | aureport --file –summary

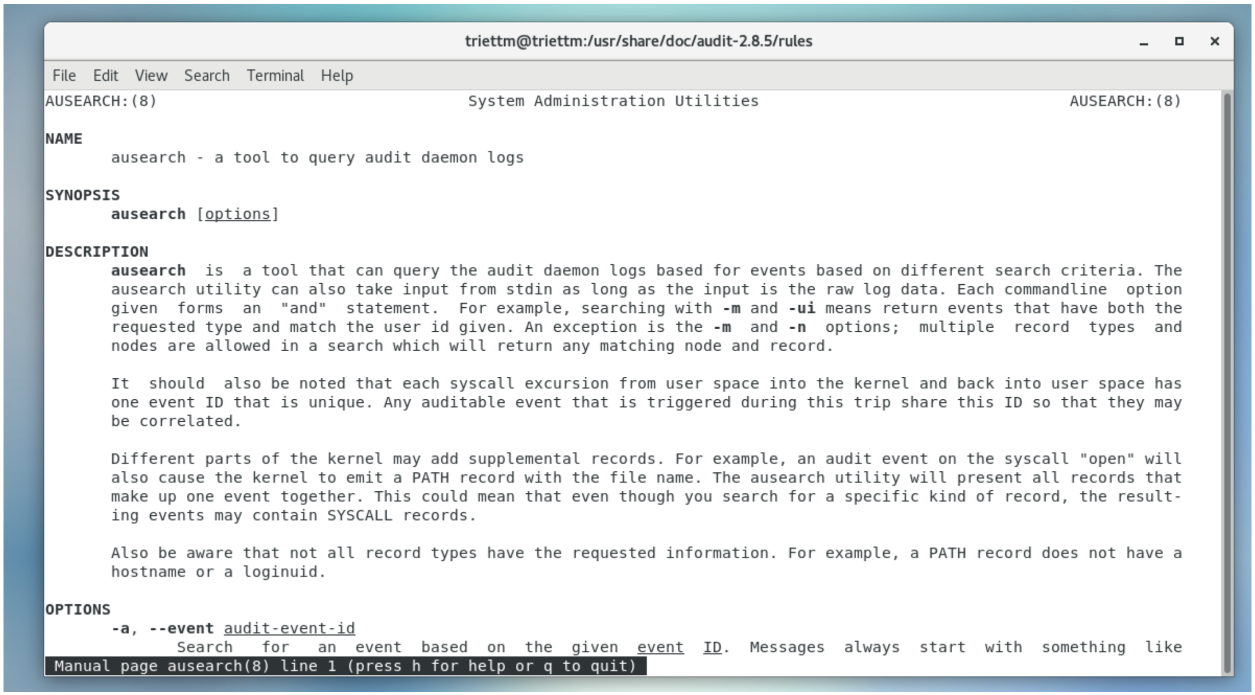

triettm@triettm:/usr/share/doc/audit-2.8.5/rules
File Edit View Search Terminal Help

```
[root@triettm rules]# ausearch --key access --raw | aureport --file --summary

File Summary Report
===========================
total  file
===========================
<no events of interest were found>

[root@triettm rules]#
```

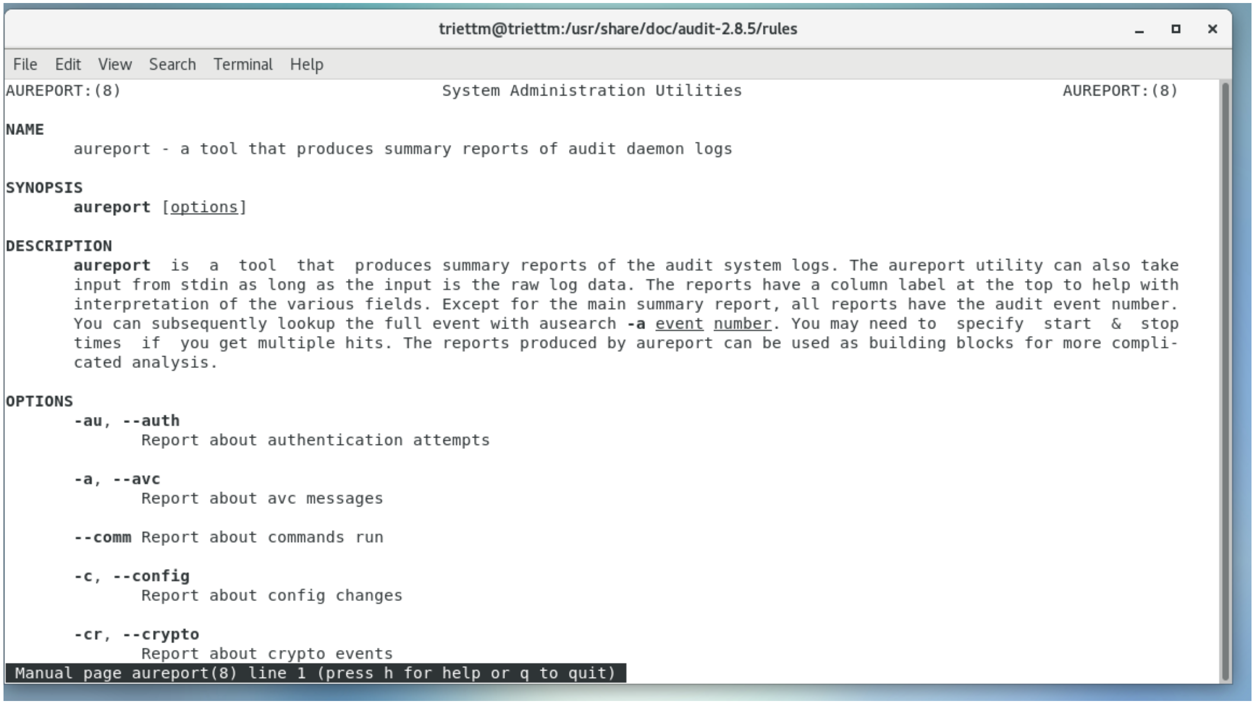
aureport –anomaly



```
[root@triettm rules]# aureport --anomaly

Anomaly Report
=========================================
# date time type exe term host auid event
=========================================
1. 01/05/2023 11:27:36 ANOM_PROMISCUOUS /usr/sbin/libvirtd (none) ? -1 116
2. 02/27/2023 13:35:15 ANOM_PROMISCUOUS /usr/sbin/libvirtd (none) ? -1 117
3. 02/27/2023 15:34:23 ANOM_PROMISCUOUS /usr/sbin/libvirtd (none) ? -1 115
[root@triettm rules]# 
```

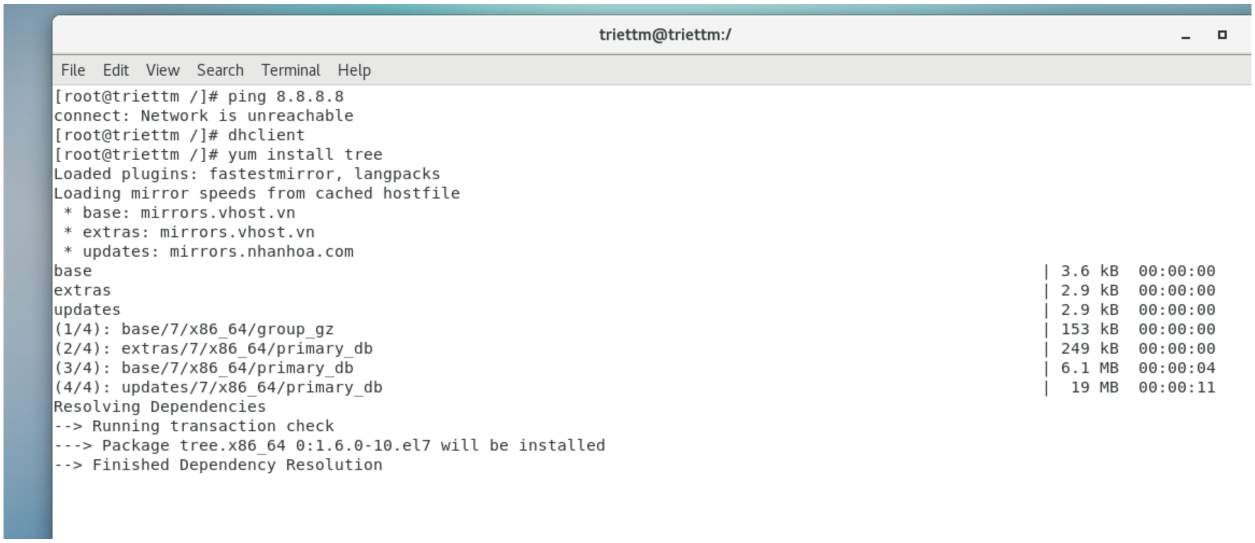

triettm@triettm:/usr/share/doc/audit-2.8.5/rules
File Edit View Search Terminal Help

```
AUSEARCH:(8)                          System Administration Utilities                          AUSEARCH:(8)

NAME
       ausearch - a tool to query audit daemon logs

SYNOPSIS
       ausearch [options]

DESCRIPTION
       ausearch  is  a tool that can query the audit daemon logs based for events based on different search criteria. The
       ausearch utility can also take input from stdin as long as the input is the raw log data. Each commandline  option
       given  forms  an  "and"  statement.  For example, searching with -m and -ui means return events that have both the
       requested type and match the user id given. An exception is the -m  and -n  options;  multiple  record  types  and
       nodes are allowed in a search which will return any matching node and record.

       It  should  also be noted that each syscall excursion from user space into the kernel and back into user space has
       one event ID that is unique. Any auditable event that is triggered during this trip share this ID so that they may
       be correlated.

       Different parts of the kernel may add supplemental records. For example, an audit event on the syscall "open" will
       also cause the kernel to emit a PATH record with the file name. The ausearch utility will present all records that
       make up one event together. This could mean that even though you search for a specific kind of record, the result-
       ing events may contain SYSCALL records.

       Also be aware that not all record types have the requested information. For example, a PATH record does not have a
       hostname or a loginuid.

OPTIONS
       -a, --event audit-event-id
              Search   for   an  event  based  on  the  given  event  ID.  Messages  always  start  with  something  like
 Manual page ausearch(8) line 1 (press h for help or q to quit)
```


triettm@triettm:/usr/share/doc/audit-2.8.5/rules
File Edit View Search Terminal Help

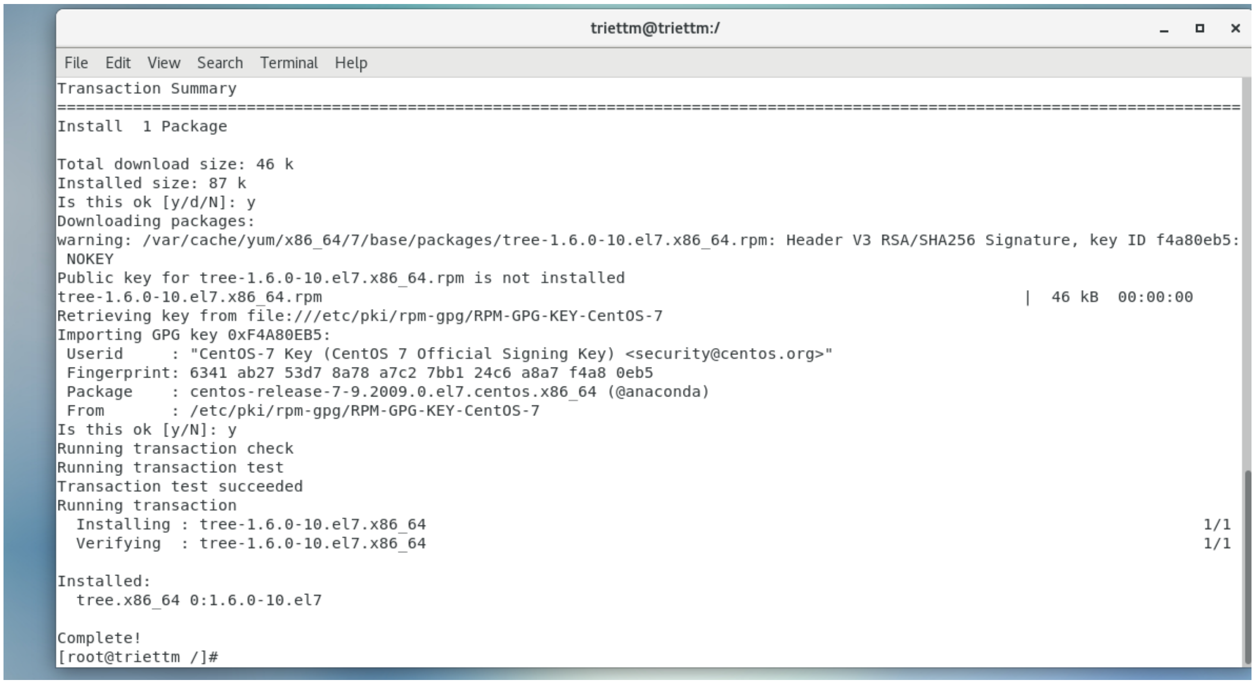
```
AUREPORT:(8)                          System Administration Utilities                          AUREPORT:(8)

NAME
       aureport - a tool that produces summary reports of audit daemon logs

SYNOPSIS
       aureport [options]

DESCRIPTION
       aureport  is  a  tool  that  produces summary reports of the audit system logs. The aureport utility can also take
       input from stdin as long as the input is the raw log data. The reports have a column label at the top to help with
       interpretation of the various fields. Except for the main summary report, all reports have the audit event number.
       You can subsequently lookup the full event with ausearch -a event number. You may need to  specify  start  &  stop
       times  if  you get multiple hits. The reports produced by aureport can be used as building blocks for more compli-
       cated analysis.

OPTIONS
       -au, --auth
              Report about authentication attempts

       -a, --avc
              Report about avc messages

       --comm Report about commands run

       -c, --config
              Report about config changes

       -cr, --crypto
              Report about crypto events
 Manual page aureport(8) line 1 (press h for help or q to quit)
```

Visualizing directories and files

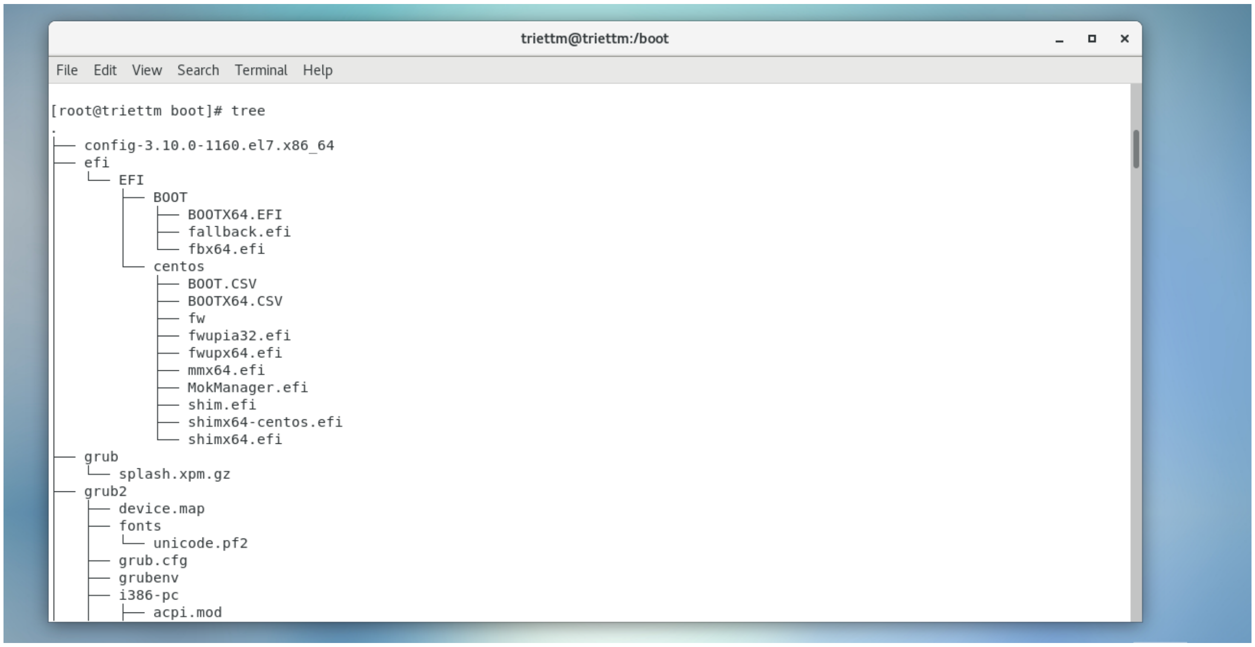


```
[root@triettm /]# ping 8.8.8.8
connect: Network is unreachable
[root@triettm /]# dhclient
[root@triettm /]# yum install tree
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.vhost.vn
 * extras: mirrors.vhost.vn
 * updates: mirrors.nhanhoa.com
base                                                                                     | 3.6 kB  00:00:00
extras                                                                                   | 2.9 kB  00:00:00
updates                                                                                  | 2.9 kB  00:00:00
(1/4): base/7/x86_64/group_gz                                                            | 153 kB  00:00:00
(2/4): extras/7/x86_64/primary_db                                                        | 249 kB  00:00:00
(3/4): base/7/x86_64/primary_db                                                          | 6.1 MB  00:00:04
(4/4): updates/7/x86_64/primary_db                                                       |  19 MB  00:00:11
Resolving Dependencies
--> Running transaction check
---> Package tree.x86_64 0:1.6.0-10.el7 will be installed
--> Finished Dependency Resolution
```

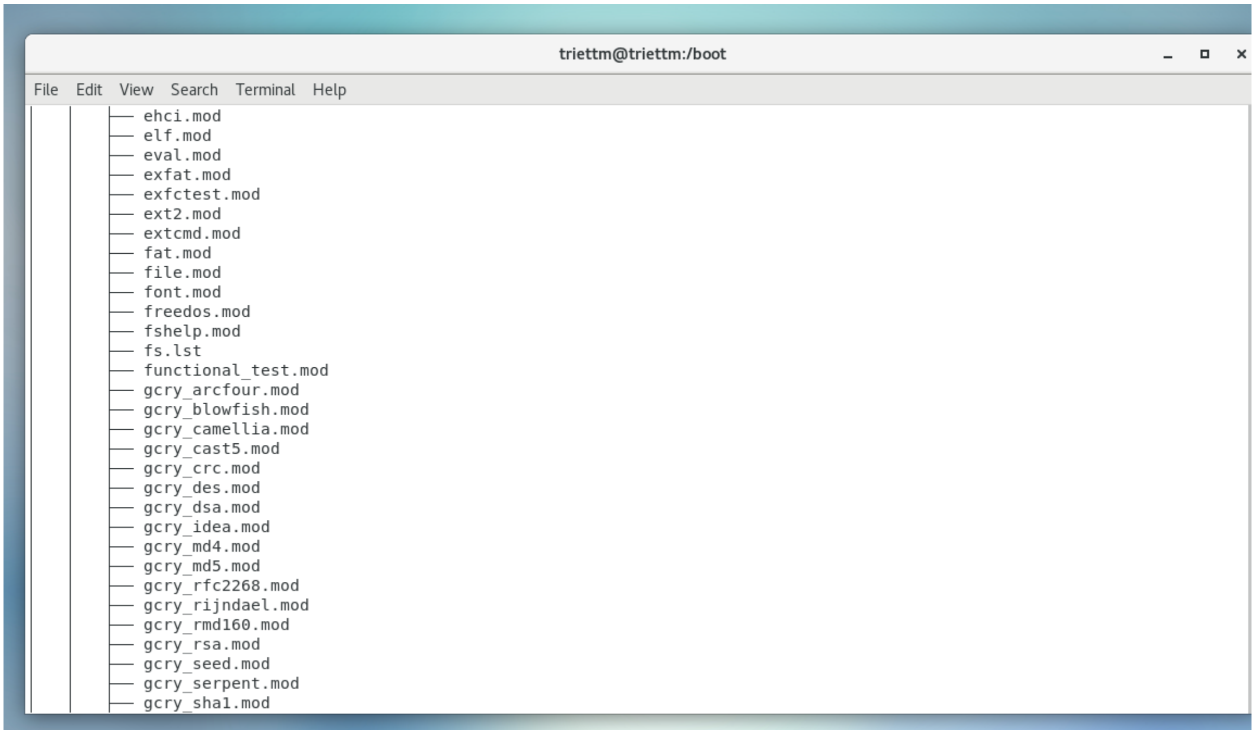
Using yum to install package tree



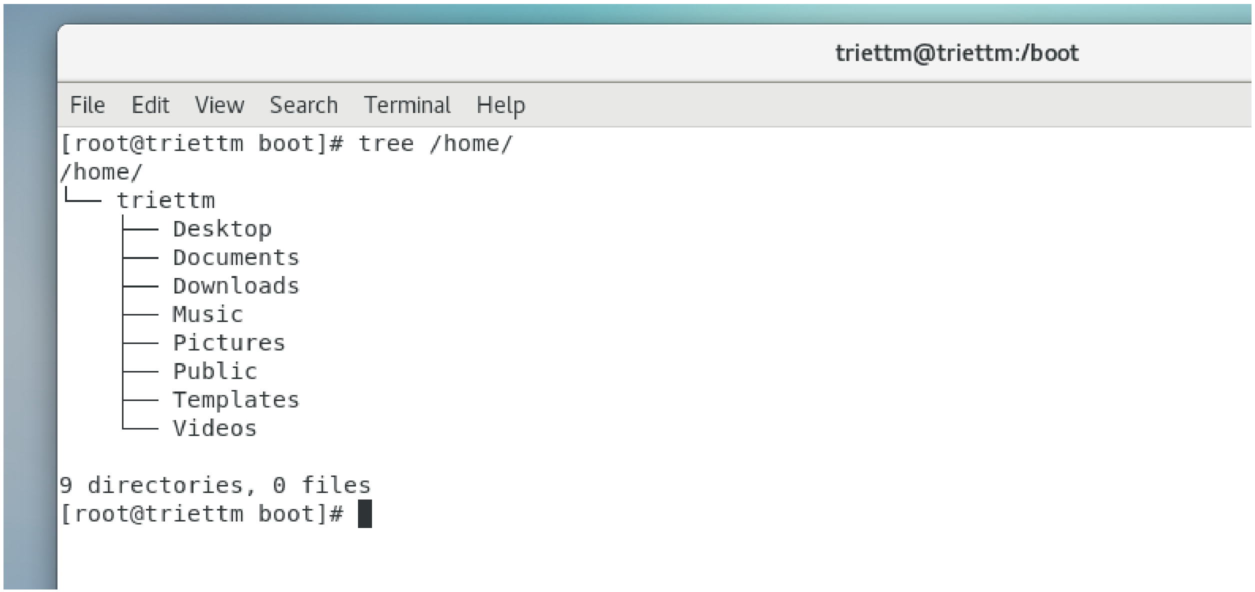
```
Transaction Summary
==========================================================================================================================
Install  1 Package

Total download size: 46 k
Installed size: 87 k
Is this ok [y/d/N]: y
Downloading packages:
warning: /var/cache/yum/x86_64/7/base/packages/tree-1.6.0-10.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID f4a80eb5:
 NOKEY
Public key for tree-1.6.0-10.el7.x86_64.rpm is not installed
tree-1.6.0-10.el7.x86_64.rpm                                                             |  46 kB  00:00:00
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid     : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint: 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a8 0eb5
 Package    : centos-release-7-9.2009.0.el7.centos.x86_64 (@anaconda)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]: y
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : tree-1.6.0-10.el7.x86_64                                                                         1/1
  Verifying  : tree-1.6.0-10.el7.x86_64                                                                         1/1

Installed:
  tree.x86_64 0:1.6.0-10.el7

Complete!
[root@triettm /]#
```



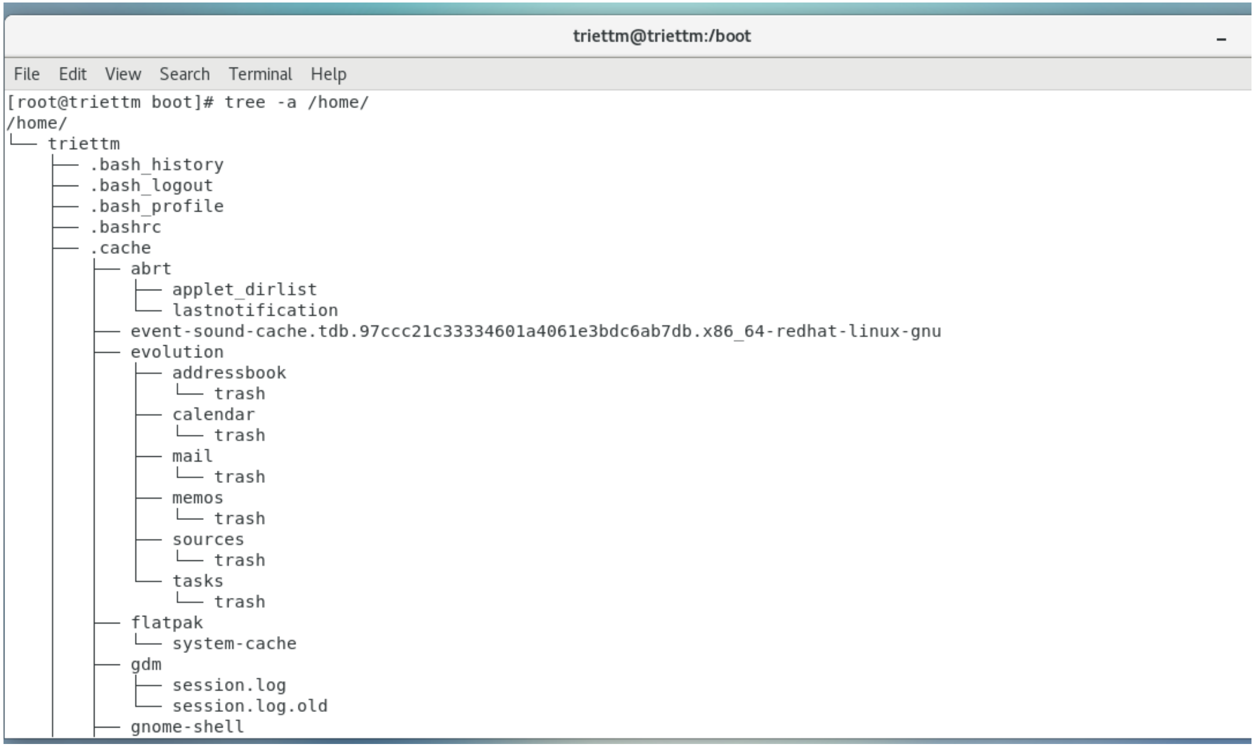
```
[root@triettm boot]# tree
.
├── config-3.10.0-1160.el7.x86_64
├── efi
│   └── EFI
│       ├── BOOT
│       │   ├── BOOTX64.EFI
│       │   ├── fallback.efi
│       │   └── fbx64.efi
│       └── centos
│           ├── BOOT.CSV
│           ├── BOOTX64.CSV
│           ├── fw
│           ├── fwupia32.efi
│           ├── fwupx64.efi
│           ├── mmx64.efi
│           ├── MokManager.efi
│           ├── shim.efi
│           ├── shimx64-centos.efi
│           └── shimx64.efi
├── grub
│   └── splash.xpm.gz
├── grub2
│   ├── device.map
│   ├── fonts
│   │   └── unicode.pf2
│   ├── grub.cfg
│   ├── grubenv
│   ├── i386-pc
│   │   ├── acpi.mod
```



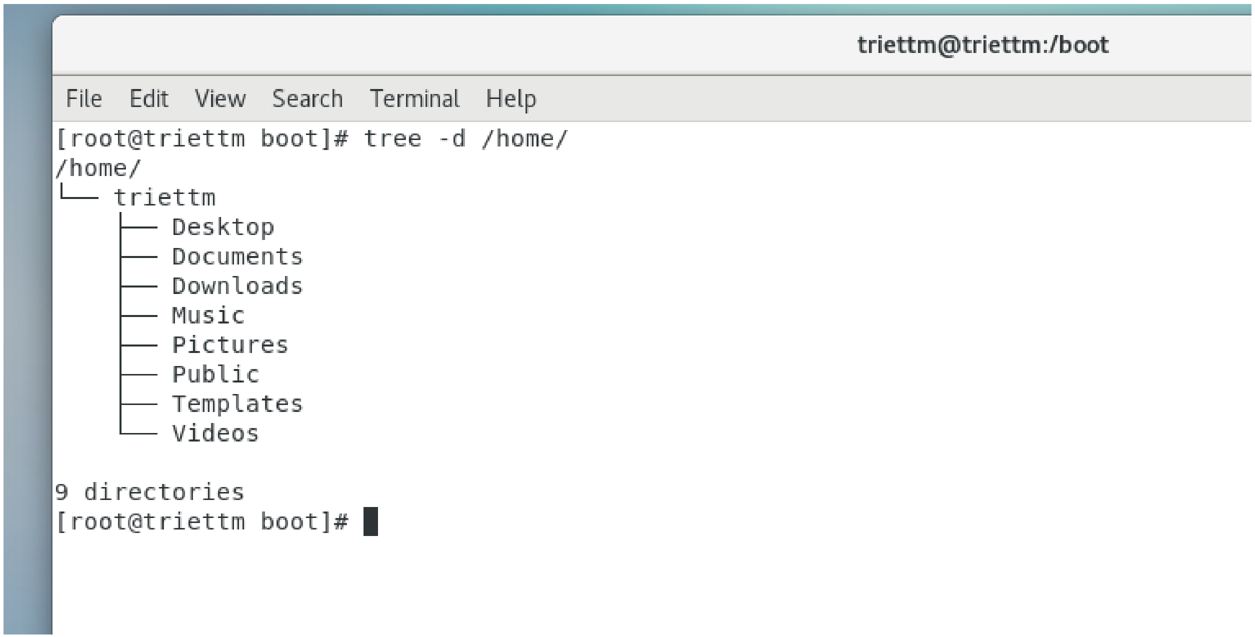
```
│   │   ├── ehci.mod
│   │   ├── elf.mod
│   │   ├── eval.mod
│   │   ├── exfat.mod
│   │   ├── exfctest.mod
│   │   ├── ext2.mod
│   │   ├── extcmd.mod
│   │   ├── fat.mod
│   │   ├── file.mod
│   │   ├── font.mod
│   │   ├── freedos.mod
│   │   ├── fshelp.mod
│   │   ├── fs.lst
│   │   ├── functional_test.mod
│   │   ├── gcry_arcfour.mod
│   │   ├── gcry_blowfish.mod
│   │   ├── gcry_camellia.mod
│   │   ├── gcry_cast5.mod
│   │   ├── gcry_crc.mod
│   │   ├── gcry_des.mod
│   │   ├── gcry_dsa.mod
│   │   ├── gcry_idea.mod
│   │   ├── gcry_md4.mod
│   │   ├── gcry_md5.mod
│   │   ├── gcry_rfc2268.mod
│   │   ├── gcry_rijndael.mod
│   │   ├── gcry_rmd160.mod
│   │   ├── gcry_rsa.mod
│   │   ├── gcry_seed.mod
│   │   ├── gcry_serpent.mod
│   │   ├── gcry_sha1.mod
```



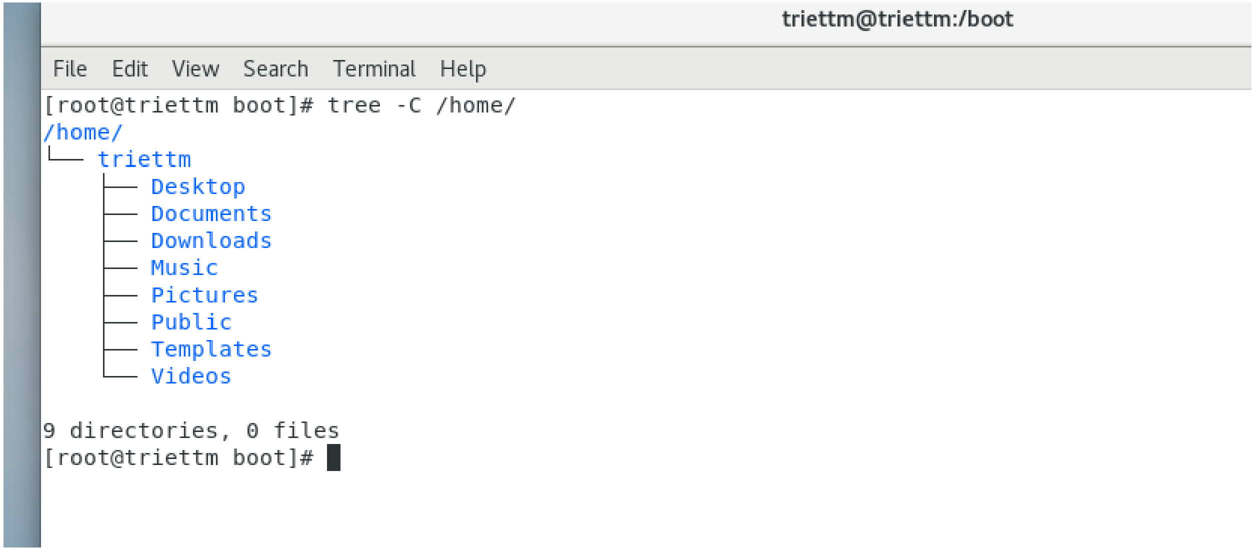
```
[root@triettm boot]# tree /home/
/home/
└── triettm
    ├── Desktop
    ├── Documents
    ├── Downloads
    ├── Music
    ├── Pictures
    ├── Public
    ├── Templates
    └── Videos

9 directories, 0 files
[root@triettm boot]# 
```



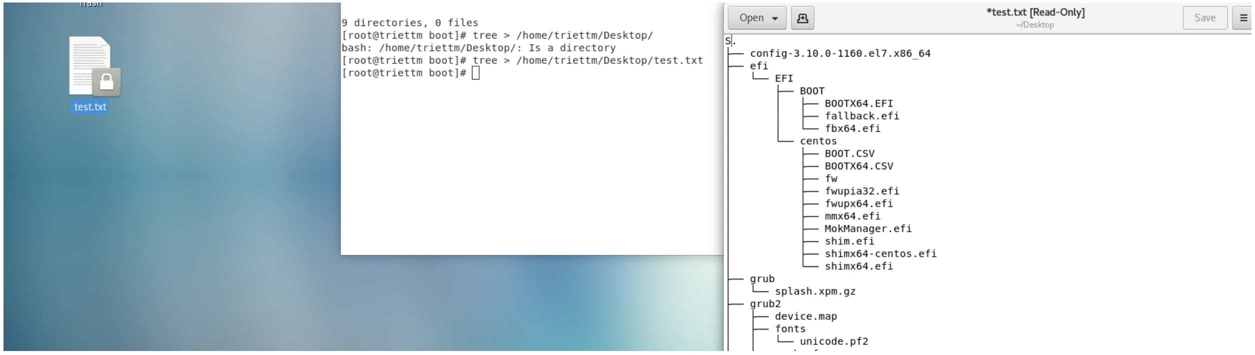
```
[root@triettm boot]# tree -a /home/
/home/
└── triettm
    ├── .bash_history
    ├── .bash_logout
    ├── .bash_profile
    ├── .bashrc
    ├── .cache
    │   ├── abrt
    │   │   ├── applet_dirlist
    │   │   └── lastnotification
    │   ├── event-sound-cache.tdb.97ccc21c33334601a4061e3bdc6ab7db.x86_64-redhat-linux-gnu
    │   ├── evolution
    │   │   ├── addressbook
    │   │   │   └── trash
    │   │   ├── calendar
    │   │   │   └── trash
    │   │   ├── mail
    │   │   │   └── trash
    │   │   ├── memos
    │   │   │   └── trash
    │   │   ├── sources
    │   │   │   └── trash
    │   │   └── tasks
    │   │       └── trash
    │   ├── flatpak
    │   │   └── system-cache
    │   ├── gdm
    │   │   ├── session.log
    │   │   └── session.log.old
    │   ├── gnome-shell
```



```
[root@triettm boot]# tree -d /home/
/home/
└── triettm
    ├── Desktop
    ├── Documents
    ├── Downloads
    ├── Music
    ├── Pictures
    ├── Public
    ├── Templates
    └── Videos

9 directories
[root@triettm boot]# 
```

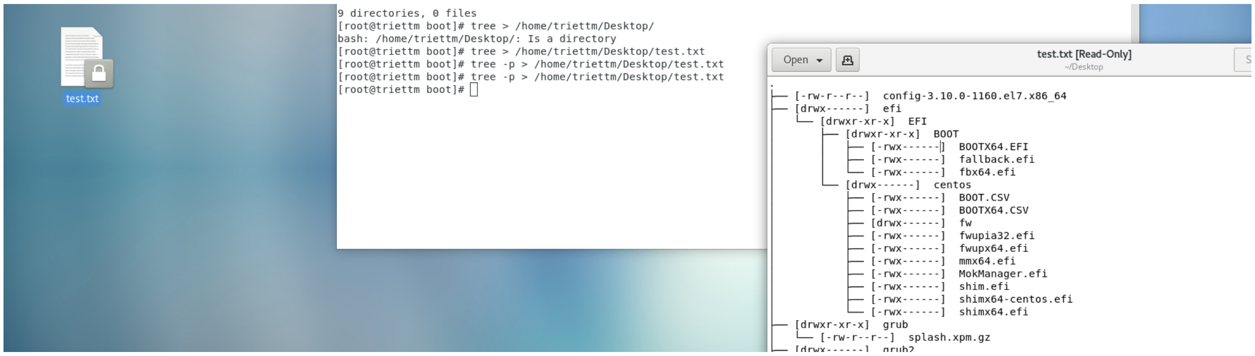


```
[root@triettm boot]# tree -C /home/
/home/
└── triettm
    ├── Desktop
    ├── Documents
    ├── Downloads
    ├── Music
    ├── Pictures
    ├── Public
    ├── Templates
    └── Videos

9 directories, 0 files
[root@triettm boot]# 
```



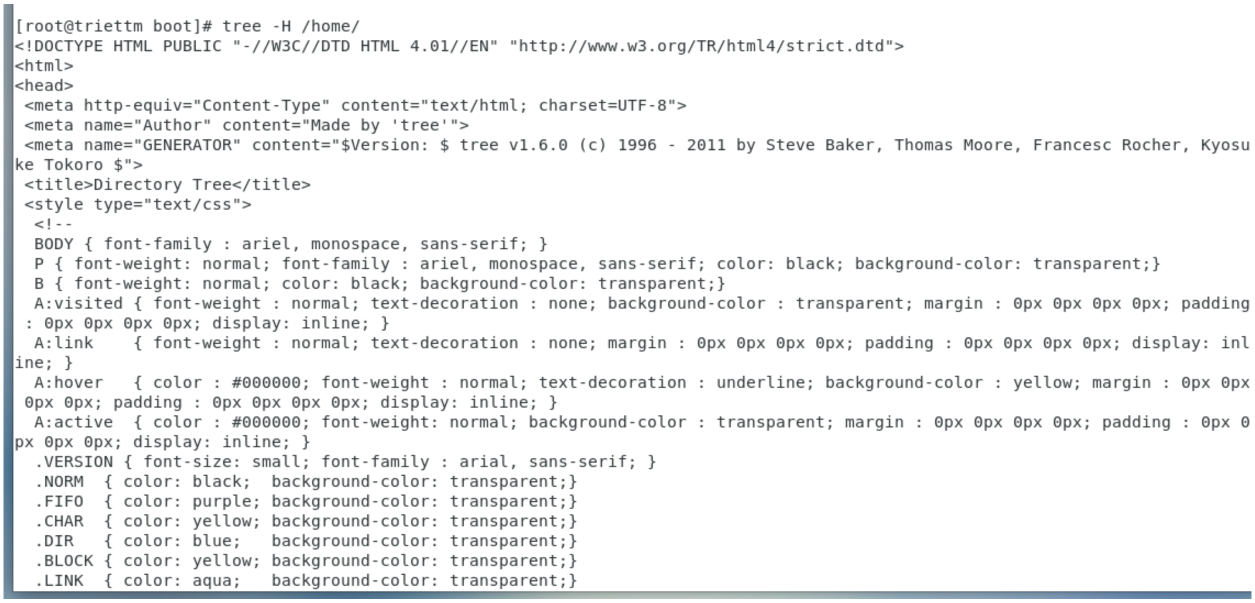
```
9 directories, 0 files
[root@triettm boot]# tree > /home/triettm/Desktop/
bash: /home/triettm/Desktop/: Is a directory
[root@triettm boot]# tree > /home/triettm/Desktop/test.txt
[root@triettm boot]# 
```

```
S.
├── config-3.10.0-1160.el7.x86_64
├── efi
│   └── EFI
│       ├── BOOT
│       │   ├── BOOTX64.EFI
│       │   ├── fallback.efi
│       │   └── fbx64.efi
│       └── centos
│           ├── BOOT.CSV
│           ├── BOOTX64.CSV
│           ├── fw
│           ├── fwupia32.efi
│           ├── fwupx64.efi
│           ├── mmx64.efi
│           ├── MokManager.efi
│           ├── shim.efi
│           ├── shimx64-centos.efi
│           └── shimx64.efi
├── grub
│   └── splash.xpm.gz
├── grub2
│   ├── device.map
│   ├── fonts
│   │   └── unicode.pf2
```

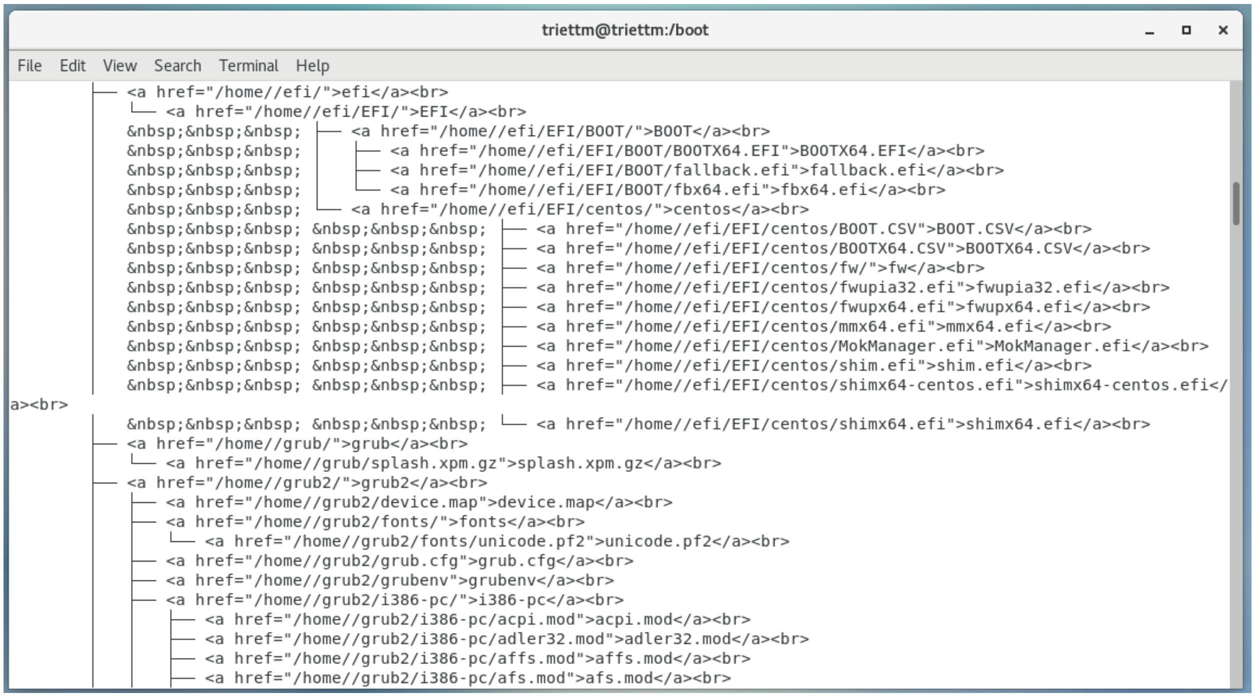


```
9 directories, 0 files
[root@triettm boot]# tree > /home/triettm/Desktop/
bash: /home/triettm/Desktop/: Is a directory
[root@triettm boot]# tree > /home/triettm/Desktop/test.txt
[root@triettm boot]# tree -p > /home/triettm/Desktop/test.txt
[root@triettm boot]# tree -p > /home/triettm/Desktop/test.txt
[root@triettm boot]# 
```

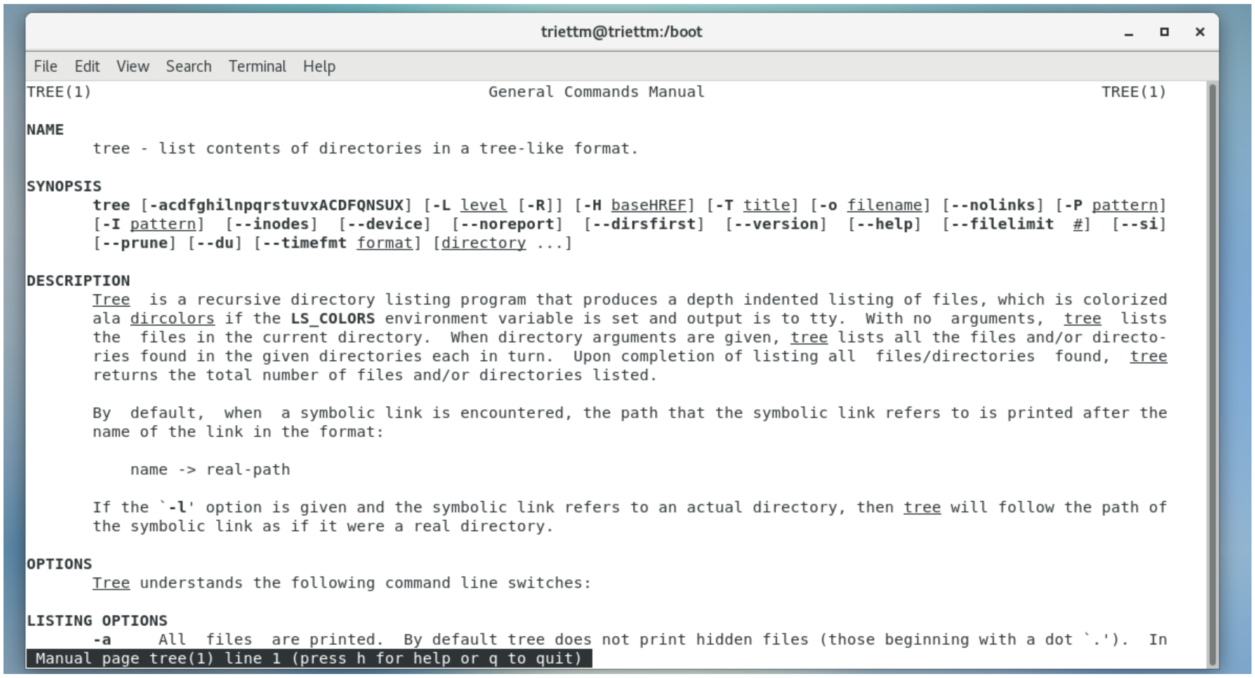
```
.
├── [-rw-r--r--]  config-3.10.0-1160.el7.x86_64
├── [drwx------]  efi
│   └── [drwxr-xr-x]  EFI
│       ├── [drwxr-xr-x]  BOOT
│       │   ├── [-rwx------]  BOOTX64.EFI
│       │   ├── [-rwx------]  fallback.efi
│       │   └── [-rwx------]  fbx64.efi
│       └── [drwx------]  centos
│           ├── [-rwx------]  BOOT.CSV
│           ├── [-rwx------]  BOOTX64.CSV
│           ├── [drwx------]  fw
│           ├── [-rwx------]  fwupia32.efi
│           ├── [-rwx------]  fwupx64.efi
│           ├── [-rwx------]  mmx64.efi
│           ├── [-rwx------]  MokManager.efi
│           ├── [-rwx------]  shim.efi
│           ├── [-rwx------]  shimx64-centos.efi
│           └── [-rwx------]  shimx64.efi
├── [drwxr-xr-x]  grub
│   └── [-rw-r--r--]  splash.xpm.gz
├── [drwx------]  grub2
```



```
[root@triettm boot]# tree -H /home/
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
 <meta name="Author" content="Made by 'tree'">
 <meta name="GENERATOR" content="$Version: $ tree v1.6.0 (c) 1996 - 2011 by Steve Baker, Thomas Moore, Francesc Rocher, Kyosu
ke Tokoro $">
 <title>Directory Tree</title>
 <style type="text/css">
  <!--
  BODY { font-family : ariel, monospace, sans-serif; }
  P { font-weight: normal; font-family : ariel, monospace, sans-serif; color: black; background-color: transparent;}
  B { font-weight: normal; color: black; background-color: transparent;}
  A:visited { font-weight : normal; text-decoration : none; background-color : transparent; margin : 0px 0px 0px 0px; padding
 : 0px 0px 0px 0px; display: inline; }
  A:link    { font-weight : normal; text-decoration : none; margin : 0px 0px 0px 0px; padding : 0px 0px 0px 0px; display: inl
ine; }
  A:hover   { color : #000000; font-weight : normal; text-decoration : underline; background-color : yellow; margin : 0px 0px
 0px 0px; padding : 0px 0px 0px 0px; display: inline; }
  A:active  { color : #000000; font-weight: normal; background-color : transparent; margin : 0px 0px 0px 0px; padding : 0px 0
px 0px 0px; display: inline; }
  .VERSION { font-size: small; font-family : arial, sans-serif; }
  .NORM  { color: black;  background-color: transparent;}
  .FIFO  { color: purple; background-color: transparent;}
  .CHAR  { color: yellow; background-color: transparent;}
  .DIR   { color: blue;   background-color: transparent;}
  .BLOCK { color: yellow; background-color: transparent;}
  .LINK  { color: aqua;   background-color: transparent;}
```



```
        ├── <a href="/home//efi/">efi</a><br>
        │   └── <a href="/home//efi/EFI/">EFI</a><br>
        │   &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/BOOT/">BOOT</a><br>
        │   &nbsp;&nbsp;&nbsp; │   ├── <a href="/home//efi/EFI/BOOT/BOOTX64.EFI">BOOTX64.EFI</a><br>
        │   &nbsp;&nbsp;&nbsp; │   ├── <a href="/home//efi/EFI/BOOT/fallback.efi">fallback.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; │   └── <a href="/home//efi/EFI/BOOT/fbx64.efi">fbx64.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; └── <a href="/home//efi/EFI/centos/">centos</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/BOOT.CSV">BOOT.CSV</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/BOOTX64.CSV">BOOTX64.CSV</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/fw/">fw</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/fwupia32.efi">fwupia32.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/fwupx64.efi">fwupx64.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/mmx64.efi">mmx64.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/MokManager.efi">MokManager.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/shim.efi">shim.efi</a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; ├── <a href="/home//efi/EFI/centos/shimx64-centos.efi">shimx64-centos.efi</
a><br>
        │   &nbsp;&nbsp;&nbsp; &nbsp;&nbsp;&nbsp; └── <a href="/home//efi/EFI/centos/shimx64.efi">shimx64.efi</a><br>
        ├── <a href="/home//grub/">grub</a><br>
        │   └── <a href="/home//grub/splash.xpm.gz">splash.xpm.gz</a><br>
        ├── <a href="/home//grub2/">grub2</a><br>
        │   ├── <a href="/home//grub2/device.map">device.map</a><br>
        │   ├── <a href="/home//grub2/fonts/">fonts</a><br>
        │   │   └── <a href="/home//grub2/fonts/unicode.pf2">unicode.pf2</a><br>
        │   ├── <a href="/home//grub2/grub.cfg">grub.cfg</a><br>
        │   ├── <a href="/home//grub2/grubenv">grubenv</a><br>
        │   ├── <a href="/home//grub2/i386-pc/">i386-pc</a><br>
        │   │   ├── <a href="/home//grub2/i386-pc/acpi.mod">acpi.mod</a><br>
        │   │   ├── <a href="/home//grub2/i386-pc/adler32.mod">adler32.mod</a><br>
        │   │   ├── <a href="/home//grub2/i386-pc/affs.mod">affs.mod</a><br>
        │   │   ├── <a href="/home//grub2/i386-pc/afs.mod">afs.mod</a><br>
```



```
TREE(1)                               General Commands Manual                              TREE(1)

NAME
       tree - list contents of directories in a tree-like format.

SYNOPSIS
       tree [-acdfghilnpqrstuvxACDFQNSUX] [-L level [-R]] [-H baseHREF] [-T title] [-o filename] [--nolinks] [-P pattern]
       [-I pattern]  [--inodes]  [--device]  [--noreport]  [--dirsfirst]  [--version]  [--help]  [--filelimit  #]  [--si]
       [--prune] [--du] [--timefmt format] [directory ...]

DESCRIPTION
       Tree  is a recursive directory listing program that produces a depth indented listing of files, which is colorized
       ala dircolors if the LS_COLORS environment variable is set and output is to tty.  With no  arguments,  tree  lists
       the  files in the current directory.  When directory arguments are given, tree lists all the files and/or directo-
       ries found in the given directories each in turn.  Upon completion of listing all  files/directories  found,  tree
       returns the total number of files and/or directories listed.

       By  default,  when  a symbolic link is encountered, the path that the symbolic link refers to is printed after the
       name of the link in the format:

           name -> real-path

       If the `-l' option is given and the symbolic link refers to an actual directory, then tree will follow the path of
       the symbolic link as if it were a real directory.

OPTIONS
       Tree understands the following command line switches:

LISTING OPTIONS
       -a     All  files  are printed.  By default tree does not print hidden files (those beginning with a dot `.').  In
 Manual page tree(1) line 1 (press h for help or q to quit)
```