

Tasks:

- cksum securecopy.txt and save the output as screen shot.

```
[root@70fdbfab089c ~]# cd mydir
[root@70fdbfab089c mydir]# cksum securecopy.txt
2766876939 488142 securecopy.txt
```

- open ~/mydir/securecopy.txt with nano OR vim editor and replace all "root" keywords with yourname and exit the nano.

Using vim

```
:%s/root/rahaf/g
```

to make sure search for root, and nothing appear

```
14:17:47,016 WARNING org.fedoraproject.Anaconda.Modules.Users:INFO:anaconda.
core.users:user account rahaf locked
14:17:47,016 WARNING org.fedoraproject.Anaconda.Modules.Users:INFO:program:R
unning... chpasswd -R /mnt/sysrahaf -e
14:17:47,279 WARNING org.fedoraproject.Anaconda.Modules.Users:INFO:program:R
unning... chage -R /mnt/sysrahaf -d rahaf
14:17:47,294 WARNING org.fedoraproject.Anaconda.Modules.Users:DEBUG:program:
```

again cksum securecopy.txt and save the output as screen shot and write your observation.

```
[root@70fdbfab089c mydir]# cksum securecopy.txt
3209986201 488224 securecopy.txt
```

- use the find command to find yourname.txt in your environment and save the output as screen shot.

```
[root@70fdbfab089c ~]# find . -iname rahaf.txt
./mydir/mydir2/rahaf.txt
```

- Use man page with the "useradd" command and save the output in "useradd-man.txt" using what you have learned in "stdin/stdout" lesson, then grep the word "password" from the "useradd-man.txt" you have created and take a screen shot for the grep output.

```
[root@70fdbfab089c ~]# grep password useradd-man.txt
The number of days after a password expires until the account
soon as the password has expired, and a value of -1 disables
account to turn off password aging, even though system account
has no password at all. Multiple -K options can be specified,
-p, --password PASSWORD
The encrypted password, as returned by crypt(3). The default is
to disable the password.
Note: This option is not recommended because the password (or
encrypted password) will be visible by users listing the
You should make sure the password respects the system's
password policy.
The number of days after a password has expired before the
name, same password, and same GID).
The maximum number of days a password may be used. If the
password is older than this, a password change will be forced.
The minimum number of days allowed between password changes.
Any password changes attempted sooner than this will be
The number of days warning given before a password expires. A
Shadow password suite configuration.
can't update password file
```