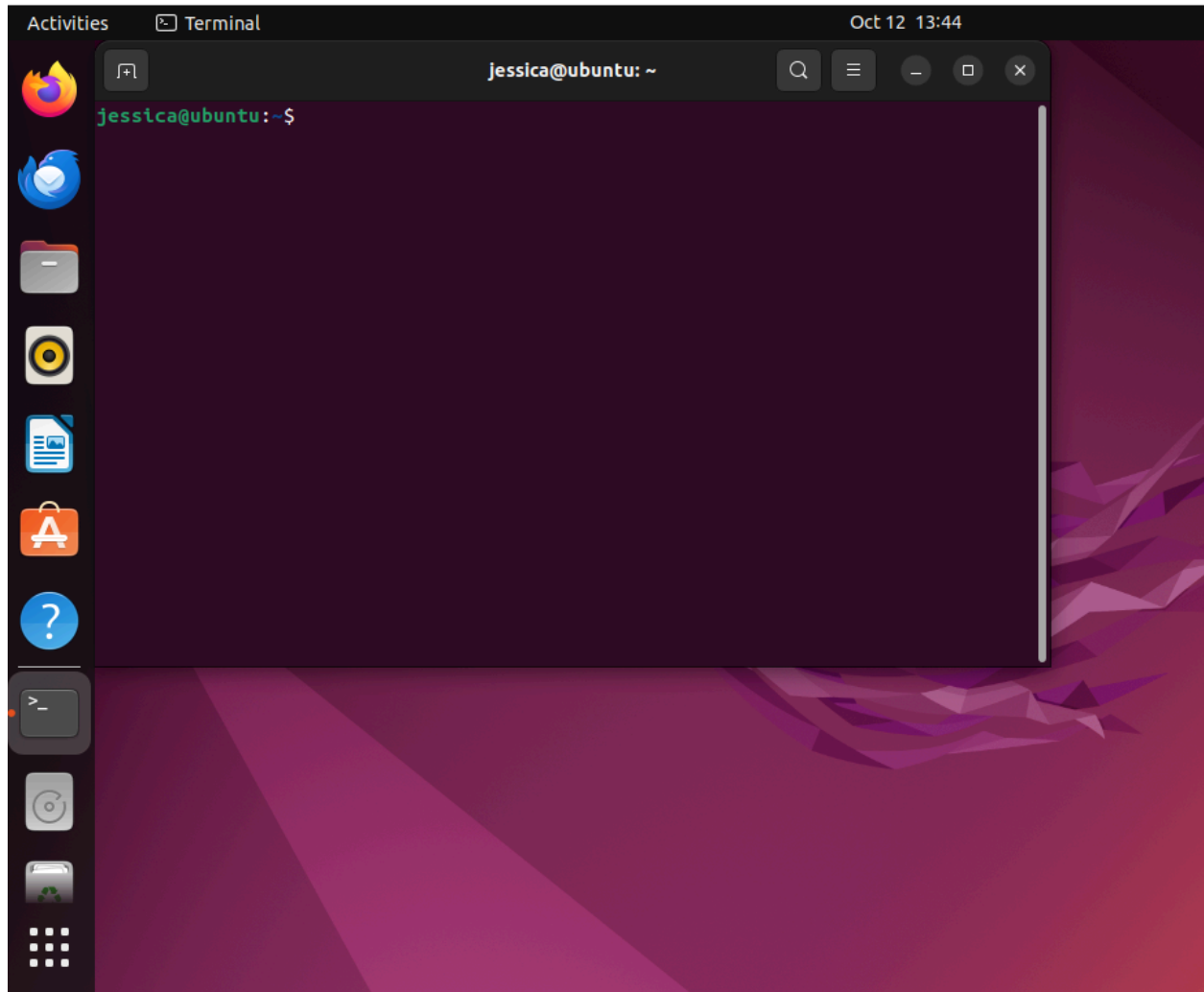


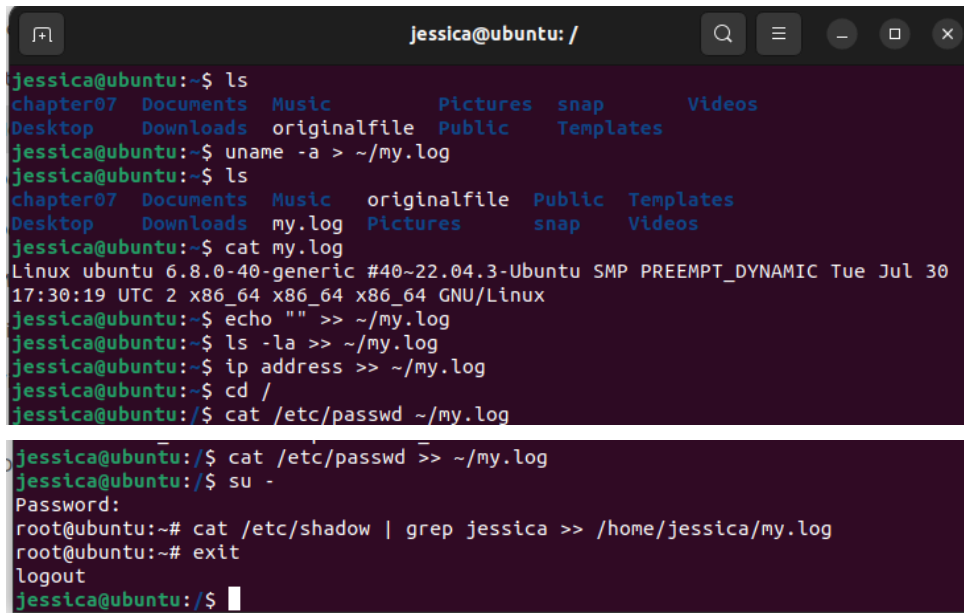
## Task 1: Collecting Live System Information

### Step 1: Launch Terminal



Successfully launched terminal on Ubuntu VM.

## Step 2: Collect System Information

A terminal window titled 'jessica@ubuntu: /' with standard window controls. It shows a series of commands and their outputs for collecting system information. The commands include 'ls', 'uname -a', 'cat', 'echo', 'ls -la', 'ip address', 'cd', and 'cat /etc/passwd'. The output of 'uname -a' shows system details like kernel version, architecture, and date. The 'cat /etc/passwd' command is run twice, once as jessica and once as root (after 'su -').

```
jessica@ubuntu:~$ ls
chapter07  Documents  Music      Pictures  snap      Videos
Desktop    Downloads  originalfile  Public    Templates

jessica@ubuntu:~$ uname -a > ~/my.log
jessica@ubuntu:~$ ls
chapter07  Documents  Music      originalfile  Public  Templates
Desktop    Downloads  my.log     Pictures      snap    Videos

jessica@ubuntu:~$ cat my.log
Linux ubuntu 6.8.0-40-generic #40~22.04.3-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 30
17:30:19 UTC 2 x86_64 x86_64 x86_64 GNU/Linux

jessica@ubuntu:~$ echo "" >> ~/my.log
jessica@ubuntu:~$ ls -la >> ~/my.log
jessica@ubuntu:~$ ip address >> ~/my.log
jessica@ubuntu:~$ cd /
jessica@ubuntu:/$ cat /etc/passwd ~/my.log

jessica@ubuntu:/$ cat /etc/passwd >> ~/my.log
jessica@ubuntu:/$ su -
Password:
root@ubuntu:~# cat /etc/shadow | grep jessica >> /home/jessica/my.log
root@ubuntu:~# exit
logout
jessica@ubuntu:/$
```

Continued on next page.

```

jessica@ubuntu:/$ cat ~/my.log
Linux ubuntu 6.8.0-40-generic #40~22.04.3-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 30
17:30:19 UTC 2 x86_64 x86_64 x86_64 GNU/Linux

total 124
drwxr-x--- 17 jessica jessica 4096 Oct 13 09:50 .
drwxr-xr-x  3 root    root    4096 Sep  1 11:16 ..
-rw-----  1 jessica jessica  539 Oct 12 15:29 .bash_history
-rw-r--r--  1 jessica jessica  220 Sep  1 11:16 .bash_logout
-rw-r--r--  1 jessica jessica 3771 Sep  1 11:16 .bashrc
drwx----- 10 jessica jessica 4096 Oct 12 14:13 .cache
drwxrwxr-x  2 jessica jessica 4096 Oct 12 15:51 chapter07
drwx----- 13 jessica jessica 4096 Oct 12 15:08 .config
drwxr-xr-x  2 jessica jessica 4096 Sep  1 11:25 Desktop
drwxr-xr-x  2 jessica jessica 4096 Sep  1 11:25 Documents
drwxr-xr-x  2 jessica jessica 4096 Sep  1 12:11 Downloads
drwx-----  2 jessica jessica 4096 Oct 13 09:49 .gnupg
drwx-----  3 jessica jessica 4096 Sep  1 11:25 .local
drwxr-xr-x  3 jessica jessica 4096 Oct 12 13:58 Music
-rw-rw-r--  1 jessica jessica  127 Oct 13 09:50 my.log

```

```

jessica@ubuntu: /
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper
:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:120:126:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
nm-openvpn:x:121:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin
/nologin
saned:x:122:129::/var/lib/saned:/usr/sbin/nologin
colord:x:123:130:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/no
login
geoclue:x:124:131::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534::/run/gnome-initial-setup:/bin/false
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
jessica:x:1000:1000:jessica,,,:/home/jessica:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
jessica:$y$9T$8S/EBDJUP6kEvHNLW1B0o.$U4WcGJaSg1tNv2RXtUqh4oEojkMfqBgdyaxlqtBf/K
0:19967:0:99999:7:::
jessica@ubuntu:/$

```

Successfully obtained system information onto my.log file.

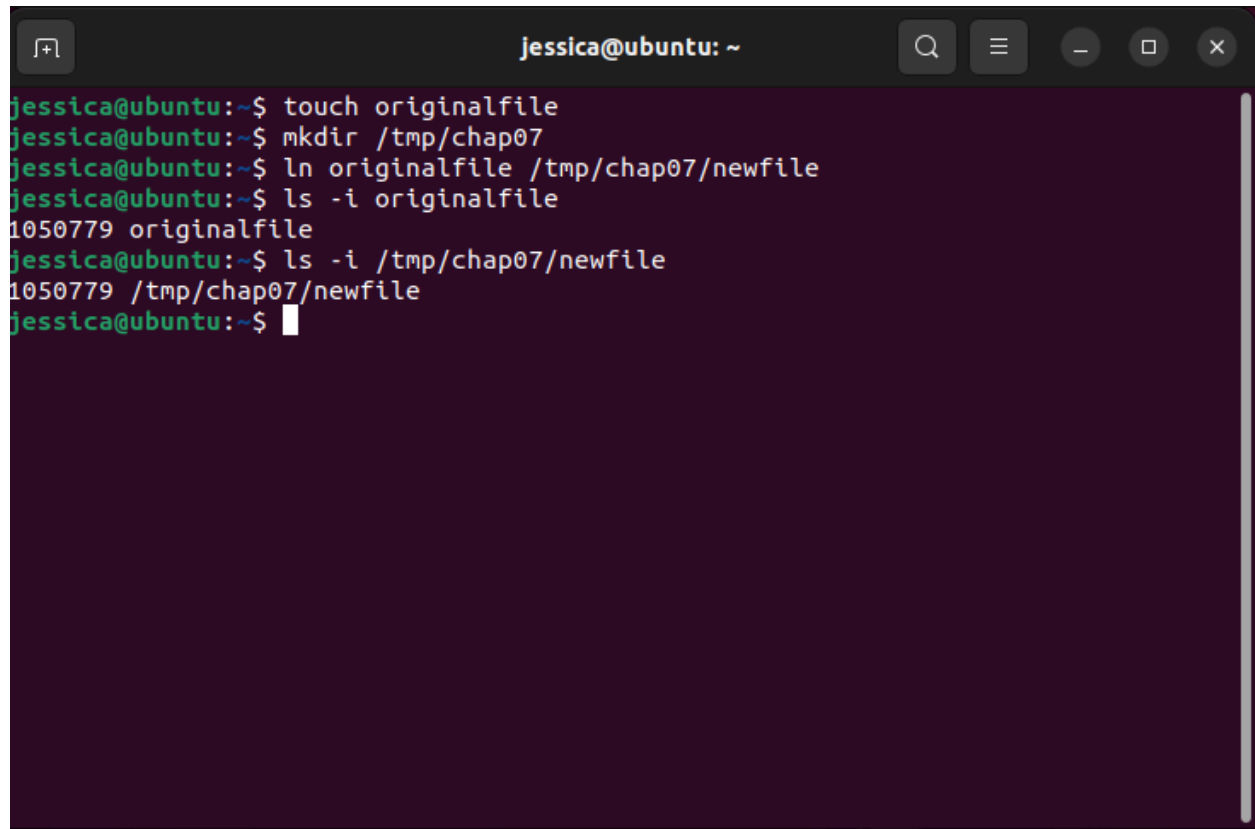
## Task 2: File Links

### Step 1: Explore Hard Links

```
jessica@ubuntu: ~  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 12:11 Downloads  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Music  
-rw-rw-r-- 1 jessica jessica 5800 Oct 12 13:55 my.log  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Pictures  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Public  
drwx----- 4 jessica jessica 4096 Sep  1 11:36 snap  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Templates  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Videos  
jessica@ubuntu:~$ cd Music  
jessica@ubuntu:~/Music$ mkdir PopTunes  
jessica@ubuntu:~/Music$ cd ..  
jessica@ubuntu:~$ ls -l  
total 44  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Desktop  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Documents  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 12:11 Downloads  
drwxr-xr-x 3 jessica jessica 4096 Oct 12 13:58 Music  
-rw-rw-r-- 1 jessica jessica 5800 Oct 12 13:55 my.log  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Pictures  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Public  
drwx----- 4 jessica jessica 4096 Sep  1 11:36 snap  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Templates  
drwxr-xr-x 2 jessica jessica 4096 Sep  1 11:25 Videos  
jessica@ubuntu:~$
```

Successfully increases the Music directory hard link count from 2 to 3 by creating a new PopTunes directory.

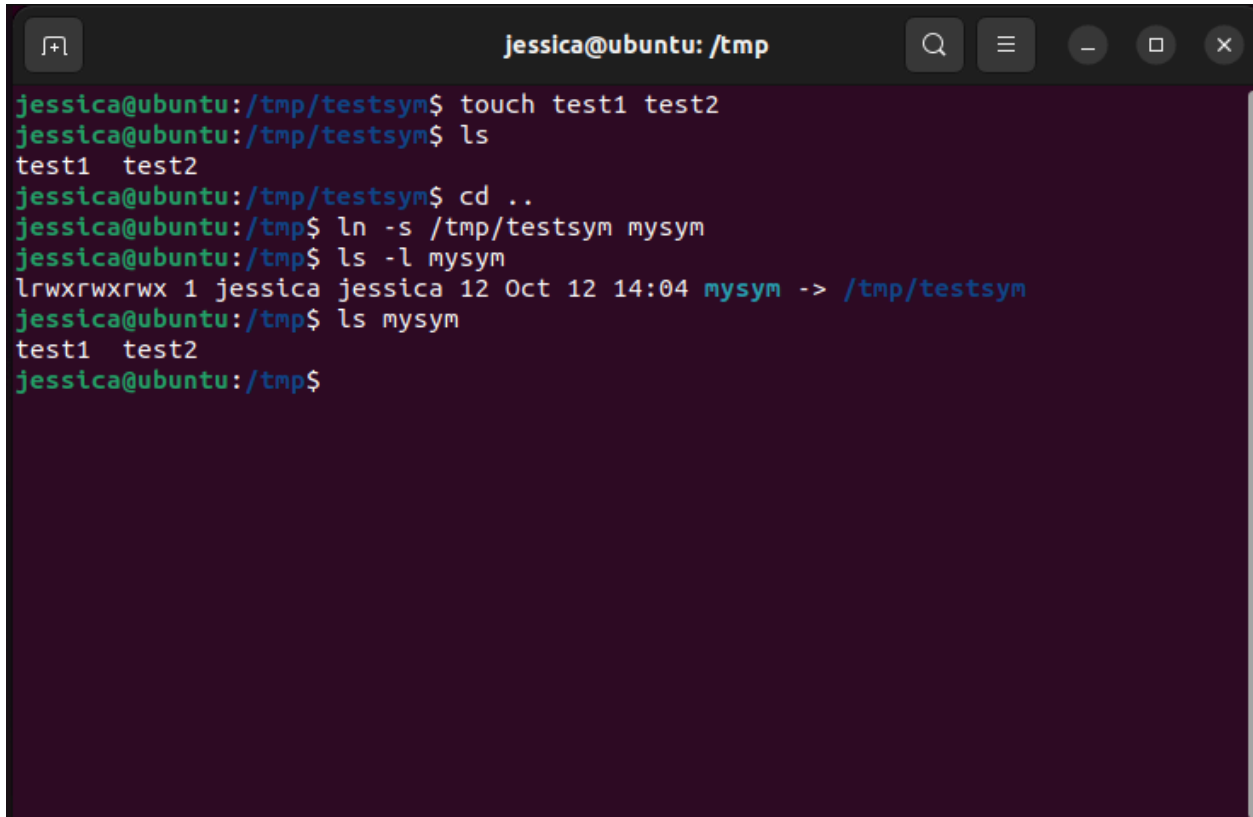
## Step 2: Create a Hard Link

A terminal window titled 'jessica@ubuntu: ~' with standard window controls. The terminal shows a series of commands and their outputs. The commands are: 'touch originalfile', 'mkdir /tmp/chap07', 'ln originalfile /tmp/chap07/newfile', 'ls -i originalfile', and 'ls -i /tmp/chap07/newfile'. The outputs are: '1050779 originalfile' and '1050779 /tmp/chap07/newfile'. The prompt returns to 'jessica@ubuntu:~\$' after the final command.

```
jessica@ubuntu:~$ touch originalfile
jessica@ubuntu:~$ mkdir /tmp/chap07
jessica@ubuntu:~$ ln originalfile /tmp/chap07/newfile
jessica@ubuntu:~$ ls -i originalfile
1050779 originalfile
jessica@ubuntu:~$ ls -i /tmp/chap07/newfile
1050779 /tmp/chap07/newfile
jessica@ubuntu:~$
```

Successfully created a hard link between the original file and the new file in the temporary chapter 7 folder. The inode numbers match, indicated that these files are hard linked.

## Step 3: Create a Symbolic Link

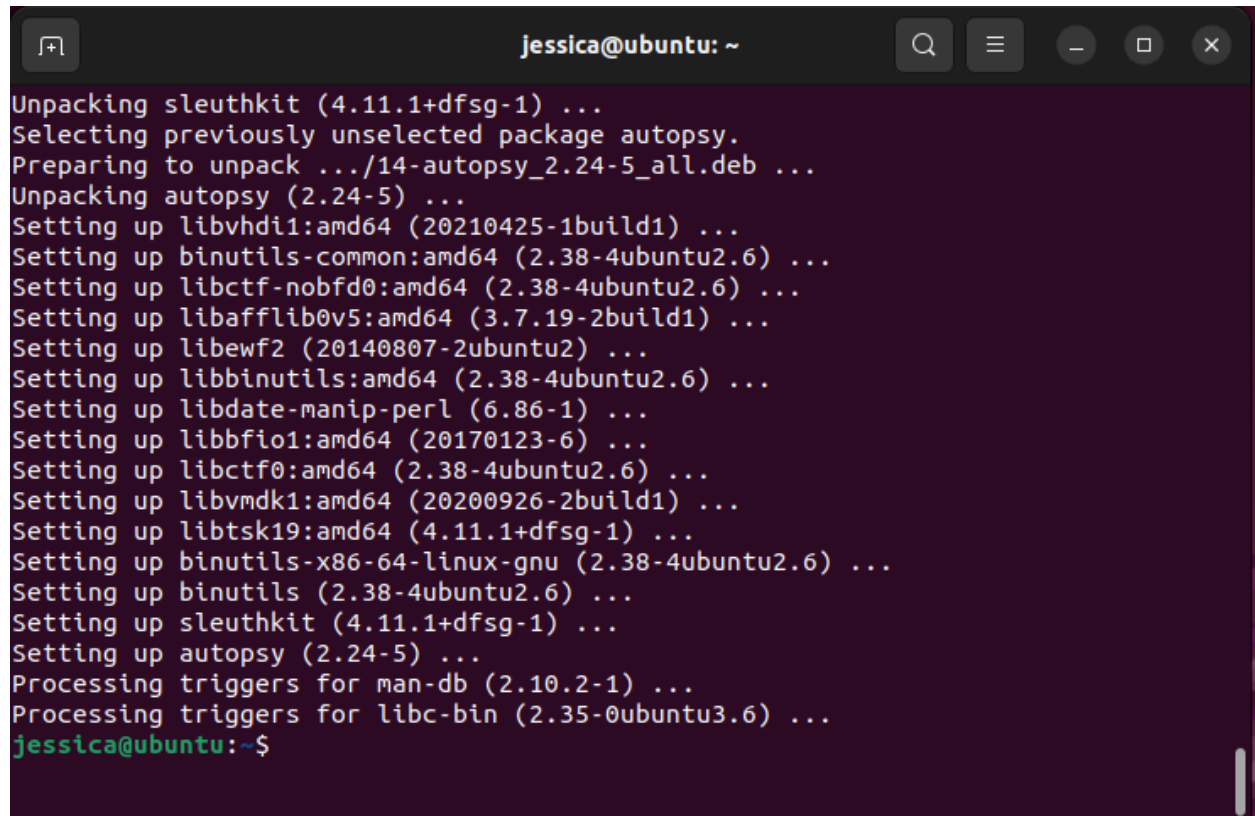
A terminal window titled 'jessica@ubuntu: /tmp' with standard window controls. The terminal shows a series of commands and their outputs. The user creates two files, 'test1' and 'test2', in the '/tmp/testsym' directory. They then move to the parent directory and create a symbolic link named 'mysym' pointing to '/tmp/testsym'. Finally, they list the contents of the 'mysym' link, which shows the same files as the original directory.

```
jessica@ubuntu:/tmp/testsym$ touch test1 test2
jessica@ubuntu:/tmp/testsym$ ls
test1  test2
jessica@ubuntu:/tmp/testsym$ cd ..
jessica@ubuntu:/tmp$ ln -s /tmp/testsym mysym
jessica@ubuntu:/tmp$ ls -l mysym
lrwxrwxrwx 1 jessica jessica 12 Oct 12 14:04 mysym -> /tmp/testsym
jessica@ubuntu:/tmp$ ls mysym
test1  test2
jessica@ubuntu:/tmp$
```

Successfully created a symbolic link to the testsym directory in the tmp folder. This link references a different place in memory and is considered a soft link (as opposed to a hard link).

### Task 3: Linux Case with Autopsy

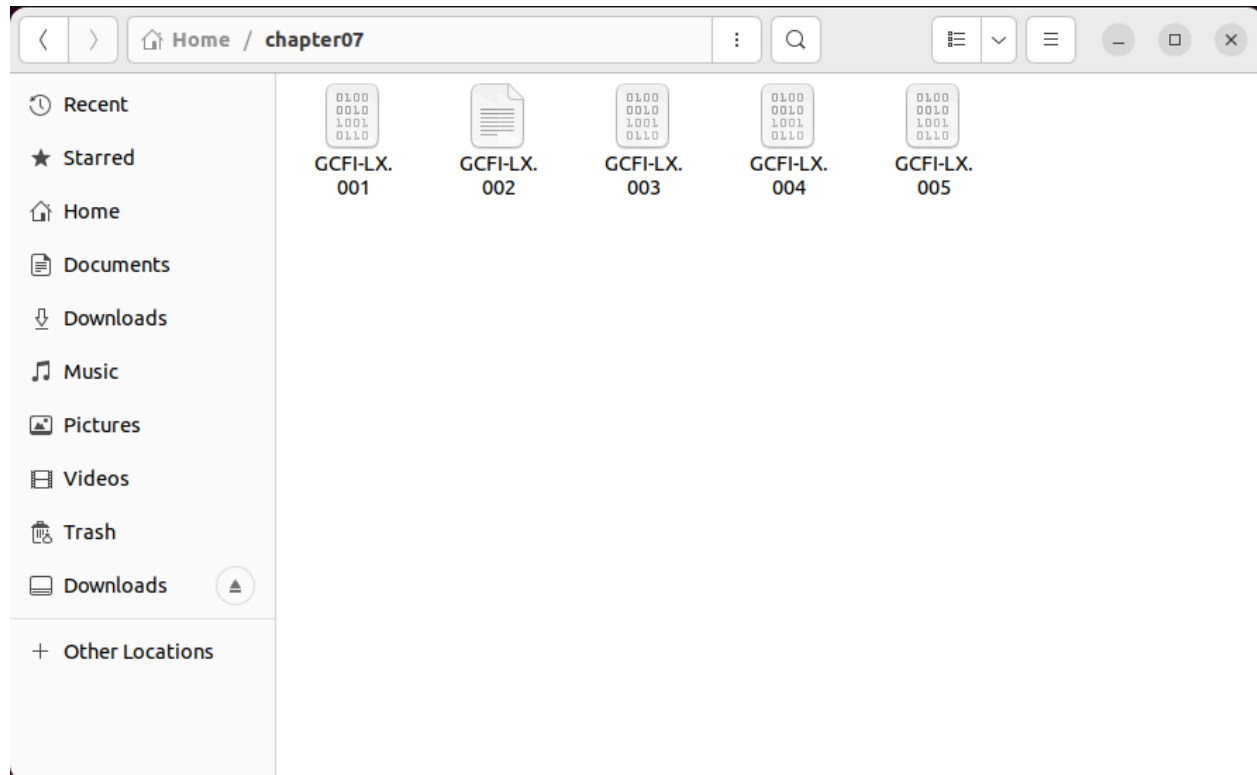
#### Step 1: Install Sleuth Kit + Autopsy

A terminal window titled 'jessica@ubuntu: ~' with standard Ubuntu window controls. The terminal output shows the installation of sleuthkit (4.11.1+dfsg-1) and autopsy (2.24-5). It lists various dependencies being set up, including libvhd1, binutils-common, libctf-nobfd0, libafflib0v5, libewf2, libbinutils, libdate-manip-perl, libbfio1, libctf0, libvmrk1, libtsk19, binutils-x86-64-linux-gnu, binutils, and sleuthkit. The process concludes with processing triggers for man-db and libc-bin, followed by the prompt 'jessica@ubuntu:~\$'.

```
jessica@ubuntu: ~  
Unpacking sleuthkit (4.11.1+dfsg-1) ...  
Selecting previously unselected package autopsy.  
Preparing to unpack .../14-autopsy_2.24-5_all.deb ...  
Unpacking autopsy (2.24-5) ...  
Setting up libvhd1:amd64 (20210425-1build1) ...  
Setting up binutils-common:amd64 (2.38-4ubuntu2.6) ...  
Setting up libctf-nobfd0:amd64 (2.38-4ubuntu2.6) ...  
Setting up libafflib0v5:amd64 (3.7.19-2build1) ...  
Setting up libewf2 (20140807-2ubuntu2) ...  
Setting up libbinutils:amd64 (2.38-4ubuntu2.6) ...  
Setting up libdate-manip-perl (6.86-1) ...  
Setting up libbfio1:amd64 (20170123-6) ...  
Setting up libctf0:amd64 (2.38-4ubuntu2.6) ...  
Setting up libvmrk1:amd64 (20200926-2build1) ...  
Setting up libtsk19:amd64 (4.11.1+dfsg-1) ...  
Setting up binutils-x86-64-linux-gnu (2.38-4ubuntu2.6) ...  
Setting up binutils (2.38-4ubuntu2.6) ...  
Setting up sleuthkit (4.11.1+dfsg-1) ...  
Setting up autopsy (2.24-5) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...  
jessica@ubuntu:~$
```

Successful installation of Sleuth kit and Autopsy after adding my user to the sudo group.

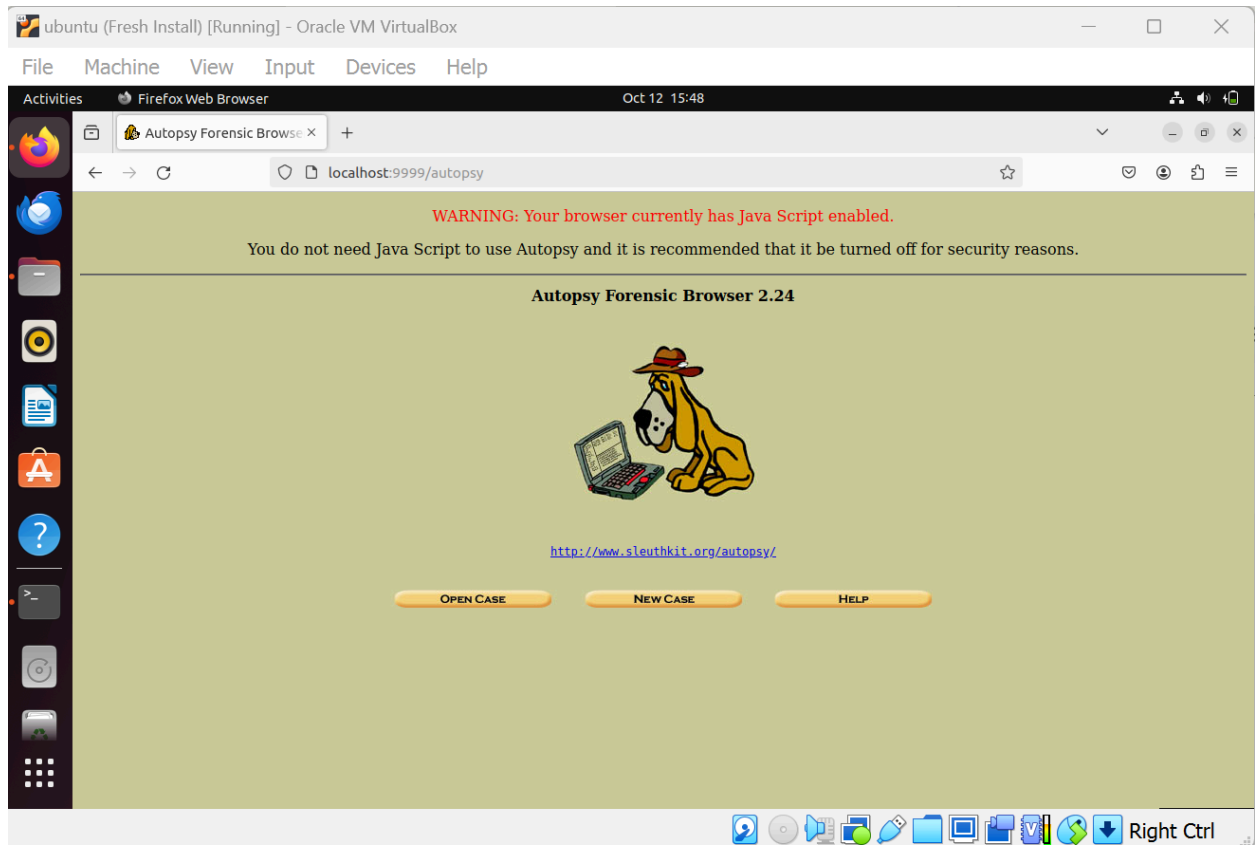
## Step 2: Get Image Files



Successfully obtained image files in Ubuntu directory.

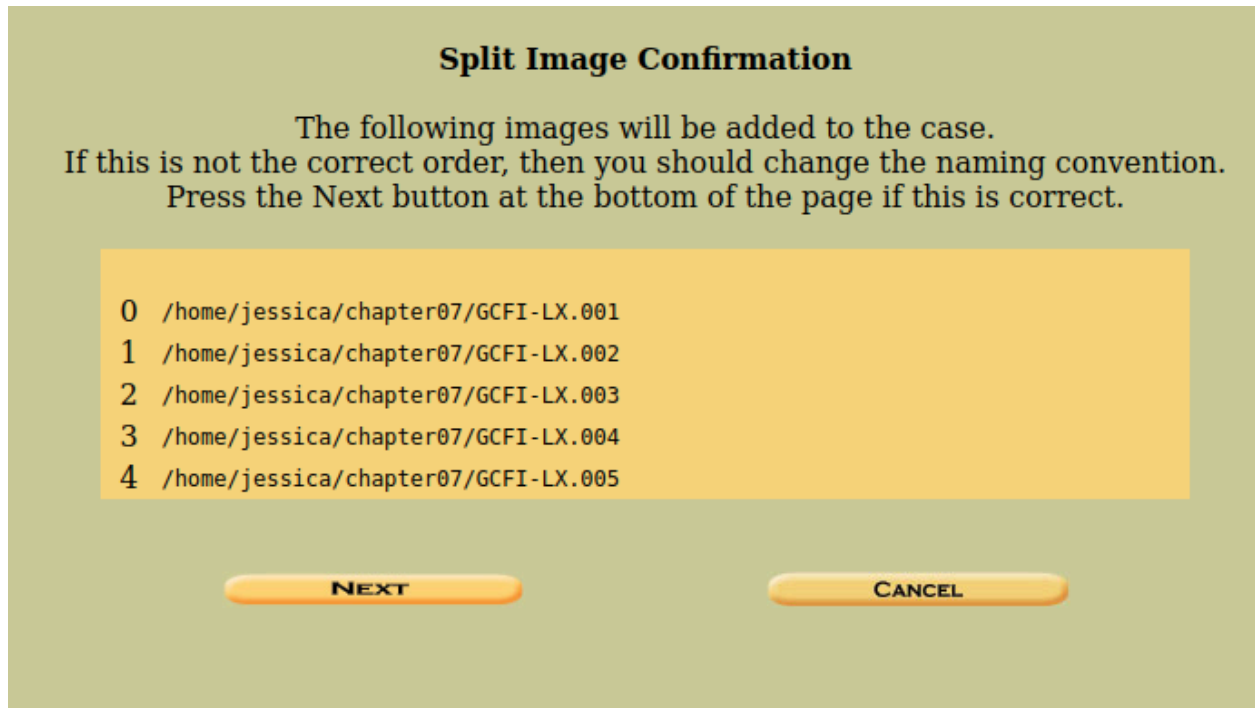


### Step 3: Start Autopsy

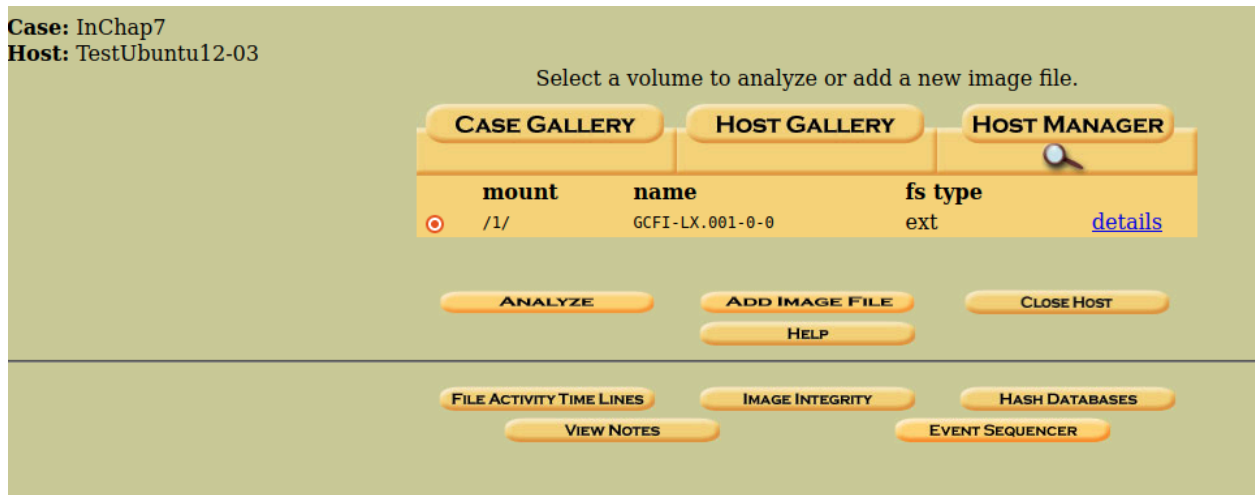


Autopsy successfully started on VM.

## Step 4: Setup the Case



**Case:** InChap7  
**Host:** TestUbuntu12-03



Successfully mounted file images.

## Step 5: Analyze the Image

Activities Firefox Web Browser Oct 12 15:54

localhost:9999/autopsy?mod=1&submod=4&case=InChap7&host=TestUbuntu12-03&inv=Jessica&vo...

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

77 occurrences of martha were found

Search Options:  
ASCII  
Case Sensitive

Fragment 236019 (Hex - Ascii)  
1: 396 (biz, martha.dax@)  
2: 855 (biz, martha.dax@)  
3: 1321 (biz, martha.dax@)  
4: 1854 (biz, martha.dax@)  
5: 2718 (biz, martha.dax@)

Fragment 236020 (Hex - Ascii)  
6: 143 (dax <martha.dax@)  
7: 3924 (martha.dax@)

Fragment 236021 (Hex - Ascii)  
8: 1228 (dax <martha.dax@)  
9: 1572 (dax <martha.dax@)  
10: 2581 (dax <martha.dax@)

Fragment 236875 (Hex - Ascii)  
11: 396 (biz, martha.dax@)  
12: 855 (biz, martha.dax@)  
13: 1321 (biz, martha.dax@)  
14: 1854 (biz, martha.dax@)  
15: 2718 (biz, martha.dax@)

Fragment 236876 (Hex - Ascii)  
16: 143 (dax <martha.dax@)  
17: 3908 (martha.dax@)

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report)

File Type: data

Fragment: 236021  
Status: Allocated  
Group: 7

ASCII Contents of Fragment 236021 in GCFI-LX.001-0-0

```

ctory.Ralph Benson <ralph.benson@superiorbicycles.biz>.Sebastian Mwangonde
<sebastian.mwangonde@superiorbicycles.biz>.Nau Tjeriko <nau.tjeriko@superiorbicycles.biz>, Chris Murphy
<chris.murphy@superiorbicycles.biz>.K...B...vx.M...vx.M..
'0|.a....0.L..y.w2XS.,*l:P..J.f=P.c.
.....v..receipt-handled.....61.&E...E....Re: [Fwd: Vacation].terrysadler
<terrysadler@goowy.com>.nau.tjeriko@superiorbicycles.biz..r..L..9.....1.63.1.E...7E....Re: Project plan for
new factory.baspen99@aol.com.nau.tjeriko@superiorbicycles.biz..}.....{,..6.....&....*l:P..J.f=P.c.
.....v..receipt-handled.....65...E...E....test.Jim Shu
<jim.shu@yahoo.com>.nau.tjeriko@superiorbicycles.biz..l.g...V.....67..E..7E....Welcome to Lycos
Mail!.Lycos Network Membership <welcome@mailbox.lycos.com>.nau.tjeriko@superiorbicycles.biz..?..[C.....&..
69.9.E.H.E..C.Re: Project plan for new factory.Sebastian Mwangonde
<sebastian.mwangonde@superiorbicycles.biz>.Ralph Benson <ralph.benson@superiorbicycles.biz>.Nau Tjeriko
<nau.tjeriko@superiorbicycles.biz>, Chris Murphy
<chris.murphy@superiorbicycles.biz>.L./...hd.K...].BK...].B..vx.M..
'0|.a....0.L..y.w2XS.,*l:P..J.f=P.c.
.....v....7..71...E...E..g.Re: Factory spec's.Martha Dax <martha.dax@superiorbicycles.biz>.Sebastian
Mwangonde <sebastian.mwangonde@superiorbicycles.biz>..jims@superiorbicycles.biz, Nau Tjeriko
<nau.tjeriko@superiorbicycles.biz>, Bart Jones <bart.jones@superiorbicycles.biz>, Chris Murphy
<chris.murphy@superiorbicycles.biz>....W...X.X....X.X.....T..73...E...E....Budget constraints.Martha
Dax <martha.dax@superiorbicycles.biz>..Chris Murphy <chris.murphy@superiorbicycles.biz>, Bob Swartz
<robert.swartz@superiorbicycles.biz>, Ralph Benson <ralph.benson@superiorbicycles.biz>, Ileen Johnson
<ileen.johnson@superiorbicycles.biz>, Bart Jones <bart.jones@superiorbicycles.biz>, Sam Clemens
<sam.clemens@superiorbicycles.biz>, Jim Shu <jim.shu@superiorbicycles.biz>, Sebastian Mwangonde
<sebastian.mwangonde@superiorbicycles.biz>, Nau Tjeriko <nau.tjeriko@superiorbicycles.biz>....b.{.....a0.
75...E...E....New computer.Denise Robinson
<denise.robinson@superiorbicycles.biz>.chris.murphy@superiorbicycles.biz.Nau Tjeriko

```

Right Ctrl

Successfully found all instances of “martha” on the images. Most of the fragments are system files or indiscernible log files. Some fragments are merely paths to different directories.