

Maria Valencia

CSC 153

Lab 7

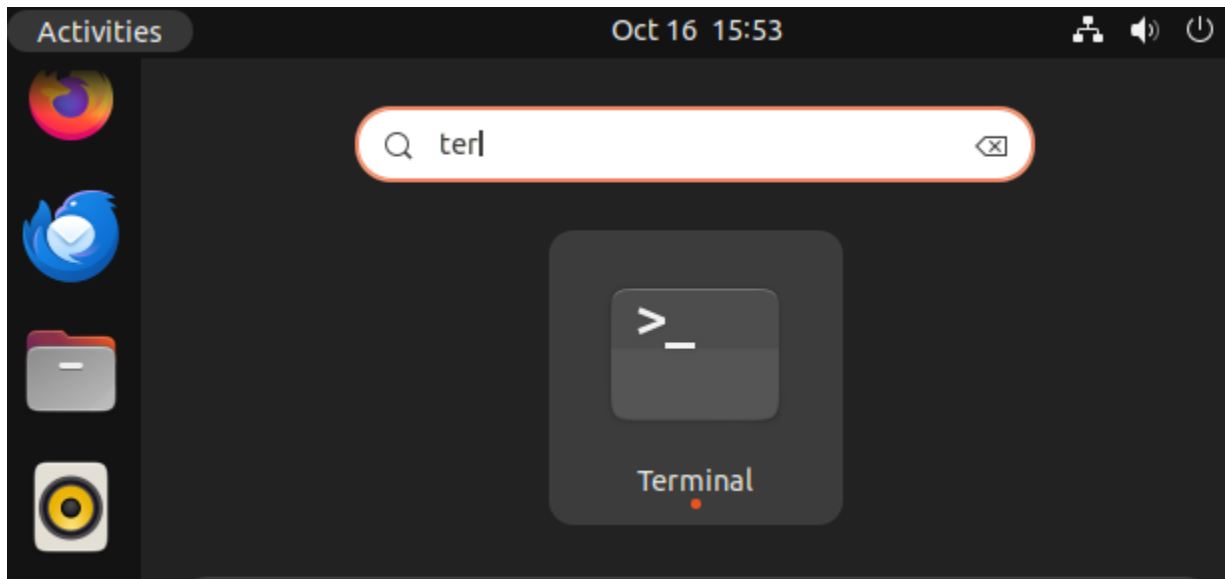
Linux Forensics

Task 1 Collecting Live System Information

In this task, I go through several Linux commands for collecting evidence on a live Linux machine using my Ubuntu/Linux VM.

Step1: Launch Terminal

I started my Linux VM and logged in. Then I started a terminal by selecting activities and then searched for terminal. Once found, I pressed the terminal button to launch the terminal.



Step 2: Collect System Information

I collected various system information and stored it in a “my.log” file from my terminal.

I found the computer name and Linux kernel version and redirected the output to the my.log file in the logged-on user’s home directory.

```
maria@ubuntu:~$ uname -a > ~/my.log
maria@ubuntu:~$
```

I determined the directory of the file system the terminal cursor is in.

```
maria@ubuntu:~$ pwd
/home/maria
maria@ubuntu:~$
```

I listed the current directory's file and folder contents.

```
maria@ubuntu:~$ ls -la
total 144
drwxr-x--- 20 maria maria 4096 Oct 16 15:57 .
drwxr-xr-x  3 root  root  4096 Sep 24 18:31 ..
-rw-----  1 maria maria 1598 Oct 10 16:32 .bash_history
-rw-r--r--  1 maria maria  220 Sep 24 18:31 .bash_logout
-rw-r--r--  1 maria maria 3771 Sep 24 18:31 .bashrc
drwx----- 11 maria maria 4096 Oct  9 18:09 .cache
drwxrwxr-x  3 maria maria 4096 Oct  2 18:53 .chef
drwx----- 14 maria maria 4096 Oct  9 18:09 .config
drwxr-xr-x  4 maria maria 4096 Oct 10 16:55 Desktop
drwxr-xr-x  2 maria maria 4096 Sep 24 18:38 Documents
drwxr-xr-x  2 maria maria 4096 Sep 24 18:38 Downloads
drwxrwxr-x  2 maria maria 4096 Oct 10 17:01 .gdb
-rw-rw-r--  1 maria maria  43 Oct 10 17:02 .gdbinit
drwx-----  2 maria maria 4096 Oct 16 15:53 .gnupg
drwxrwxr-x  3 maria maria 4096 Oct  2 19:08 .inspec
drwx-----  3 maria maria 4096 Sep 24 18:38 .local
drwxr-xr-x  2 maria maria 4096 Sep 24 18:38 Music
-rw-rw-r--  1 maria maria  126 Oct 16 15:57 my.log
drwxrwxr-x  4 maria maria 4096 Oct 10 16:26 peda
```

I appended a blank line to the end of my.log file.

```
maria@ubuntu:~$ echo "" >> ~/my.log
maria@ubuntu:~$
```

I added a section name to my.log file.

```
maria@ubuntu:~$ echo "Full Listing:" >> ~/my.log
maria@ubuntu:~$
```

I appended the current directory's file listing to the my.log file.

```
maria@ubuntu:~$ ls -la >> ~/my.log
maria@ubuntu:~$
```

I displayed the file contents of my.log to the standard output of the terminal.

```
maria@ubuntu:~$ cat ~/my.log
Linux ubuntu 6.8.0-45-generic #45~22.04.1-Ubuntu SMP PREEMPT_D
YNAMIC Wed Sep 11 15:25:05 UTC 2 x86_64 x86_64 x86_64 GNU/Linu
x

Full Listing:
total 144
drwxr-x--- 20 maria maria 4096 Oct 16 15:57 .
drwxr-xr-x  3 root  root  4096 Sep 24 18:31 ..
-rw-----  1 maria maria 1598 Oct 10 16:32 .bash_history
-rw-r--r--  1 maria maria  220 Sep 24 18:31 .bash_logout
-rw-r--r--  1 maria maria 3771 Sep 24 18:31 .bashrc
drwx----- 11 maria maria 4096 Oct  9 18:09 .cache
drwxr-xr-x  3 maria maria 4096 Oct  9 18:53 .chaf
```

I displayed the network interface information to the standard output.

```
maria@ubuntu:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UN
KNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq
_codel state UP group default qlen 1000
    link/ether 08:00:27:3f:a7:68 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic nopre
fixroute enp0s3
        valid_lft 85536sec preferred_lft 85536sec
    inet6 fe80::ada0:b158:f380:d382/64 scope link noprefixrou
te
        valid_lft forever preferred_lft forever
maria@ubuntu:~$
```

I appended the network interference information to the end of the my.log file.

```
maria@ubuntu:~$ ip address >> ~/my.log
maria@ubuntu:~$
```

I changed the directory to the root folder of the file system. Observed the slight change from ~ to / before the \$ character in the terminal.

```
maria@ubuntu:~$ cd /
maria@ubuntu:/$
```

Then I identified the current logon user.

```
maria@ubuntu:/$ whoami
maria
maria@ubuntu:/$
```

I listed all the users on the machine from the passwd file.

```
maria@ubuntu:/$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

I displayed my user account information from the passwd file.

```
maria@ubuntu:/$ cat /etc/passwd | grep maria
maria:x:1000:1000:maria,,,:/home/maria:/bin/bash
maria@ubuntu:/$
```

I appended the passwd file contents to the my.log file.

```
maria@ubuntu:/$ cat /etc/passwd >> ~/my.log
maria@ubuntu:/$
```

I displayed a detailed file listing of the shadow file.

```
maria@ubuntu:/$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1558 Sep 24 18:36 /etc/shadow
maria@ubuntu:/$
```

I switched the user to the root user using the following commands.

```
maria@ubuntu:/$ su -
Password:
root@ubuntu:~#
```

While logged in as the root user, I displayed the shadow file contents.

```
root@ubuntu:~# cat /etc/shadow
root:$y$j9T$IbU5lcK/10MSpLwNwrytF1$Jv59JoWjY6yapzebCZAw4EqLyex
1JQSNrjzrXjsX8K.:19991:0:99999:7:::
daemon:!:19977:0:99999:7:::
bin:!:19977:0:99999:7:::
sys:!:19977:0:99999:7:::
sync:!:19977:0:99999:7:::
games:!:19977:0:99999:7:::
man:!:19977:0:99999:7:::
```

I appended the shadow file contents to the my.log file.

```
root@ubuntu:~# cat /etc/shadow | grep maria >> /home/maria/my.
log
root@ubuntu:~#
```

Then I returned to the user terminal by logging out of the root session.

```
root@ubuntu:~# exit
logout
maria@ubuntu:/$
```

I checked the contents of my.log file and observed the shadow content for my user account was appended to the end of the file.

```
maria@ubuntu:/$ cat ~/my.log
Linux ubuntu 6.8.0-45-generic #45~22.04.1-Ubuntu SMP PREEMPT_D
YNAMIC Wed Sep 11 15:25:05 UTC 2 x86_64 x86_64 x86_64 GNU/Linu
x

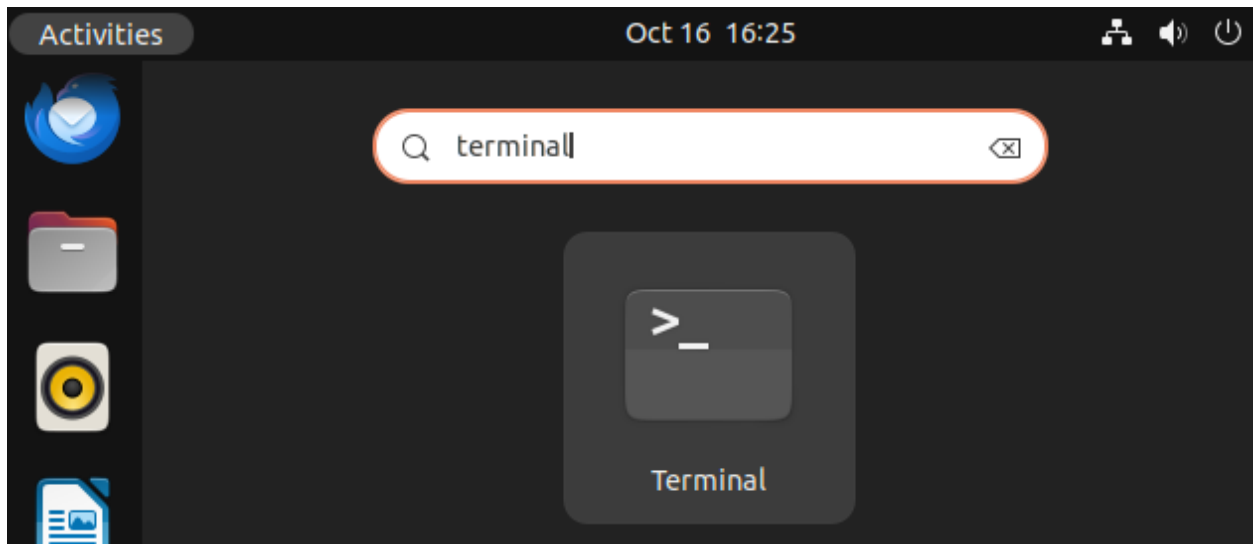
Full Listing:
total 144
drwxr-x--- 20 maria maria 4096 Oct 16 15:57 .
drwxr-xr-x  3 root  root  4096 Sep 24 18:31 ..
```

```
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
maria:x:1000:1000:maria,,,:/home/maria:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
maria:$y$j9T$XHqNw11T3WKqMJiXQ.yU1/$RngtE0UGSMsjaN9FdcBwjD59gx
ayFZQVHP.6gLoV.V8:19991:0:99999:7:::
maria@ubuntu:/$
```

Task 2 File Links

In this task, I explored symbolic links using my ubuntu VM.

Step1: Explore Hard Links



I listed the contents of the current directory including their hard link counts. I observed the hard link count for all the directories is at least 2.

```
maria@ubuntu:~$ ls -l
total 48
drwxr-xr-x 4 maria maria 4096 Oct 10 16:55 Desktop
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Documents
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Downloads
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Music
-rw-rw-r-- 1 maria maria 6113 Oct 16 16:20 my.log
drwxrwxr-x 4 maria maria 4096 Oct 10 16:26 peda
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Pictures
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Public
drwx----- 4 maria maria 4096 Sep 27 16:00 snap
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Templates
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Videos
maria@ubuntu:~$
```

I changed directories to the music folder and created a subdirectory “PopTunes”.

```
maria@ubuntu:~$ cd Music
maria@ubuntu:~/Music$ mkdir PopTunes
maria@ubuntu:~/Music$
```

I returned to the home directory and listed the directory contents including hard link counts. I observed the hard link count for Music increased by one.

```
maria@ubuntu:~$ ls -l
total 48
drwxr-xr-x 4 maria maria 4096 Oct 10 16:55 Desktop
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Documents
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Downloads
drwxr-xr-x 3 maria maria 4096 Oct 16 16:30 Music
-rw-rw-r-- 1 maria maria 6113 Oct 16 16:20 my.log
drwxrwxr-x 4 maria maria 4096 Oct 10 16:26 peda
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Pictures
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Public
drwx----- 4 maria maria 4096 Sep 27 16:00 snap
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Templates
drwxr-xr-x 2 maria maria 4096 Sep 24 18:38 Videos
maria@ubuntu:~$
```

Step 2: Create a Hard Link

I created a new file named “originalfile”.

```
maria@ubuntu:~$ touch originalfile
maria@ubuntu:~$
```

I created a subdirectory in the /tmp/folder

```
maria@ubuntu:~$ mkdir /tmp/chap07
maria@ubuntu:~$
```

I created a hard link to the originalfile in the /tmp/chap07 directory

```
maria@ubuntu:~$ ln originalfile /tmp/chap07/newfile
maria@ubuntu:~$
```

I checked the originalfile's inode number.

```
maria@ubuntu:~$ ls -li originalfile
1229686 originalfile
maria@ubuntu:~$
```

I then checked the newfile hard link inode number in the /tmp/chap07. I observed that the inode number matches originalfile.

```
maria@ubuntu:~$ ls -li /tmp/chap07/newfile
1229686 /tmp/chap07/newfile
maria@ubuntu:~$
```

Step 3: Create a Symlink

I changed directories to the /tmp folder.

```
maria@ubuntu:~$ cd /tmp
maria@ubuntu:/tmp$
```

I created a new directory testsym.

```
maria@ubuntu:/tmp$ mkdir testsym
maria@ubuntu:/tmp$
```

I changed directory to testsym.

```
maria@ubuntu:/tmp$ cd testsym
maria@ubuntu:/tmp/testsym$
```

I created two files named test1 and test2 in the testsym folder.

```
maria@ubuntu:/tmp/testsym$ touch test1 test2
maria@ubuntu:/tmp/testsym$
```

I changed directory to the /tmp folder.


```
maria@ubuntu:/tmp/testsym$ cd ..  
maria@ubuntu:/tmp$
```

I created the symbolic link mysym to the /tmp/testsym directory

```
maria@ubuntu:/tmp$ ln -s /tmp/testsym mysym  
maria@ubuntu:/tmp$
```

I listed the mysym symlink in the /tmp directory.

```
maria@ubuntu:/tmp$ ls -l mysym  
lrwxrwxrwx 1 maria maria 12 Oct 16 16:53 mysym -> /tmp/testsym  
maria@ubuntu:/tmp$
```

I listed the contents of the mysym directory. I observed that the test files are there!

```
maria@ubuntu:/tmp$ ls mysym  
1 test test1 test2  
maria@ubuntu:/tmp$
```

Task 3 Linux case with Autopsy

In this task, I installed Sleuth Kit + Autopsy on my Ubuntu VM and used the software to analyze a Linux File System.

Step1: Install Sleuth Kit + Autopsy

I logged into my Ubuntu VM and opened the terminal. I switched user to root and my regular user to the sudo. Once added, I rebooted the VM.

```
maria@ubuntu:~/Desktop$ su -  
Password:  
root@ubuntu:~# usermod -aG sudo maria  
root@ubuntu:~#
```

Once the VM rebooted, I opened another terminal and updated the system.







```
maria@ubuntu:~/Desktop$ sudo apt update -y
[sudo] password for maria:
Sorry, try again.
[sudo] password for maria:
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
```

After the updates were complete, I installed Sleuth Kit and Autopsy.

```
maria@ubuntu:~/Desktop$ sudo apt install sleuthkit autopsy -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libafflib0v5 libbfio1 libdate-manip-perl libewf2 libtsk19
  libvhdi1 libvmrk1
Suggested packages:
  mac-robber
The following NEW packages will be installed:
  autopsy libafflib0v5 libbfio1 libdate-manip-perl libewf2
  libtsk19 libvhdi1 libvmrk1 sleuthkit
0 upgraded, 9 newly installed, 0 to remove and 31 not upgraded.
Need to get 4,117 kB of archives.
After this operation, 22.2 MB of additional disk space will be used.
```

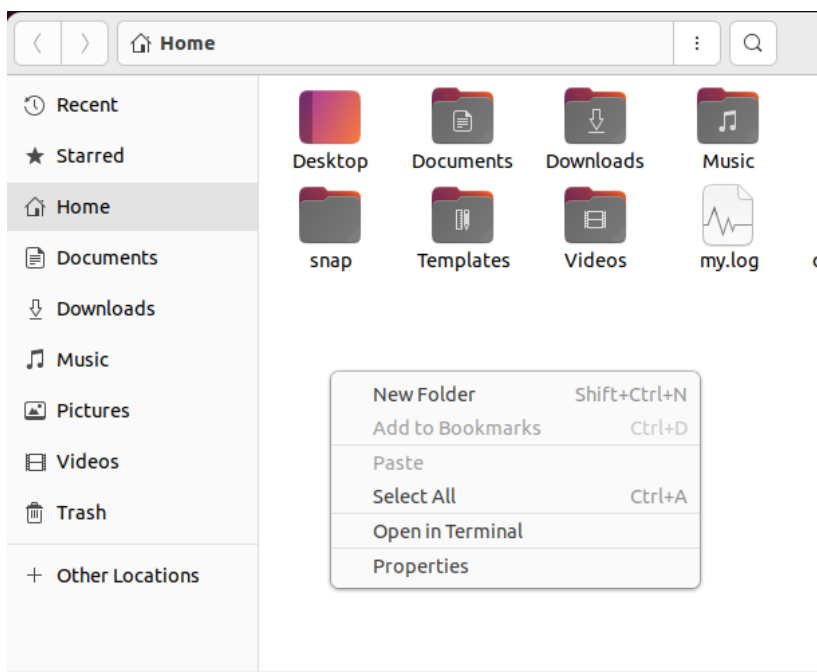
Step 2: Get Image files

On my host machine, I downloaded chapter07 .zip.file. I unzipped it and observed the exe file GCF-LX.xxx is extracted. I double clicked this WinRaR self extracting file.

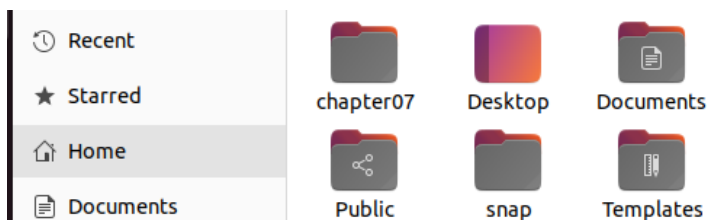
Name	Date modified	Type	Size
▼ Today			
 GCFI-LX.xxx	10/16/2024 5:39 PM	Application	1,053,897 KB
▼ A long time ago			
 GCFI-LX.001	3/11/2007 10:52 PM	001 File	665,600 KB
 GCFI-LX.002	3/11/2007 10:53 PM	002 File	665,600 KB
 GCFI-LX.003	3/11/2007 10:54 PM	003 File	665,600 KB
 GCFI-LX.004	3/11/2007 10:55 PM	004 File	665,600 KB
 GCFI-LX.005	3/11/2007 10:55 PM	005 File	502,372 KB

Back

on my Ubuntu VM, I opened the Files application, right clicked in the open folder and selected new folder.

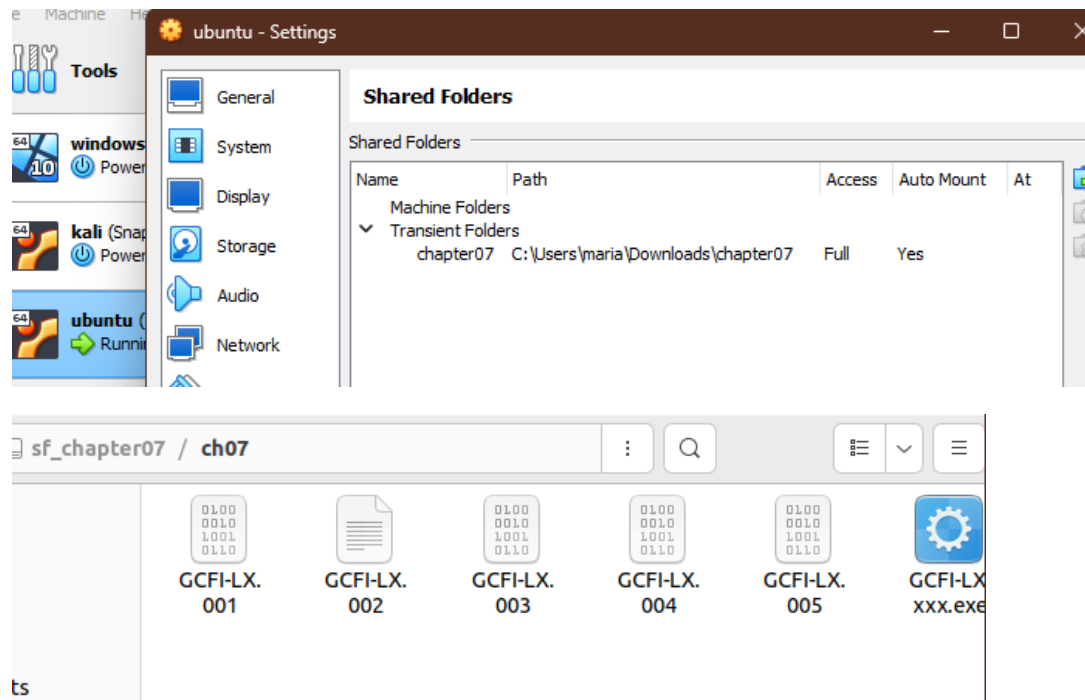


I named the folder chapter07 and opened it by double clicking it.



My drag and drop were not working, so I shared the folder with the VM by selecting the Devices menu, Shared Folders, and Shared Folder settings. Then I pressed the add folder

button, selected the folder path, used /mnt for the mount point and selected auto-mount and ok. (I then moved it from the shared folder to the appropriate folder in Ubuntu).



Step 3: Start Autopsy

Once Sleuth Kit and Autopsy have been installed, I ran the following command in my terminal to start the Autopsy browser.

```
maria@ubuntu:~/Desktop$ sudo autopsy
[sudo] password for maria:

=====
=====

Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24

=====
=====

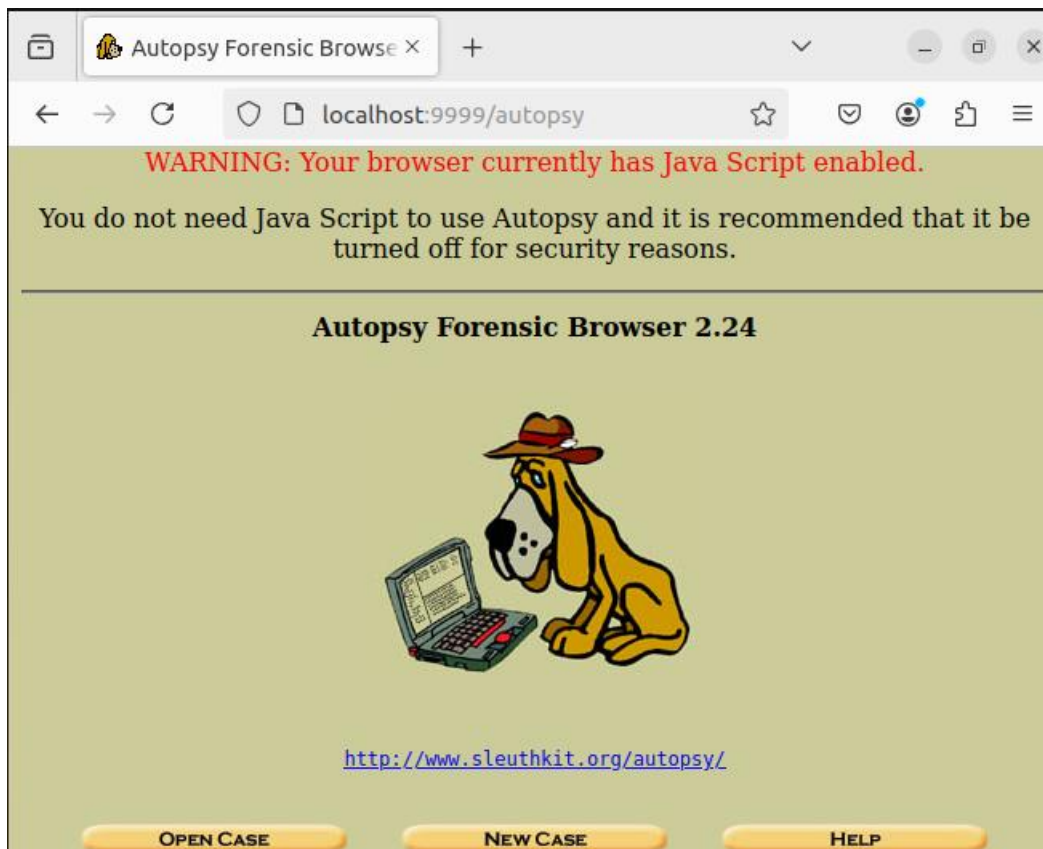
Evidence Locker: /var/lib/autopsy
Start Time: Wed Oct 16 17:59:46 2024
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

http://localhost:9999/autopsy

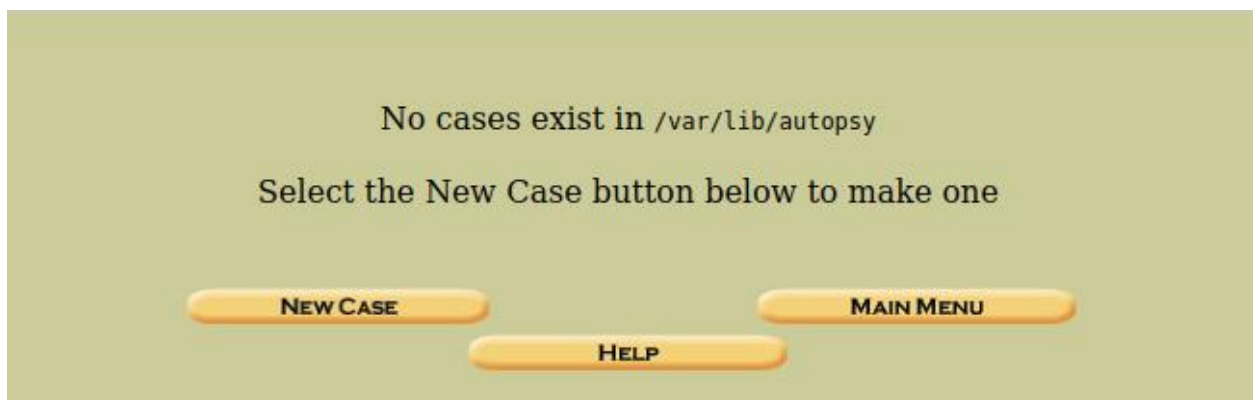
Keep this process running and use <ctrl-c> to exit
```

I opened firefox and navigated to <http://localhost:9999/autopsy>



Step 4: Setup the Case

With autopsy running in the browser, on the Ubuntu VM, I opened a new case by selecting the Open Case button on the main page. I pressed the new case button to create a new case.



I set the case name as “InChap07” and my name in the 3.a field under investigator name. Then I pressed the new case button.

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

InChap07

2. **Description:** An optional, one line description of this case.

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a.	Maria	b.	
c.		d.	
e.		f.	
g.		h.	
i.		j.	

NEW CASE CANCEL HELP

I pressed the Add Host Button to create a host for the case.

Creating Case: InChap07

Case directory (/var/lib/autopsy/InChap07/) created
Configuration file (/var/lib/autopsy/InChap07/case.aut) created

We must now create a host for this case.

Please select your name from the list: Maria ▾

ADD HOST

I entered "TestUbuntu12-03" for the Host name field and then pressed Add Host.

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

TestUbuntu12-03

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Add Host **CANCEL** **HELP**

I pressed add image on the adding host screen to add my subject image files.

Adding host: TestUbuntu12-03 to case InChap07

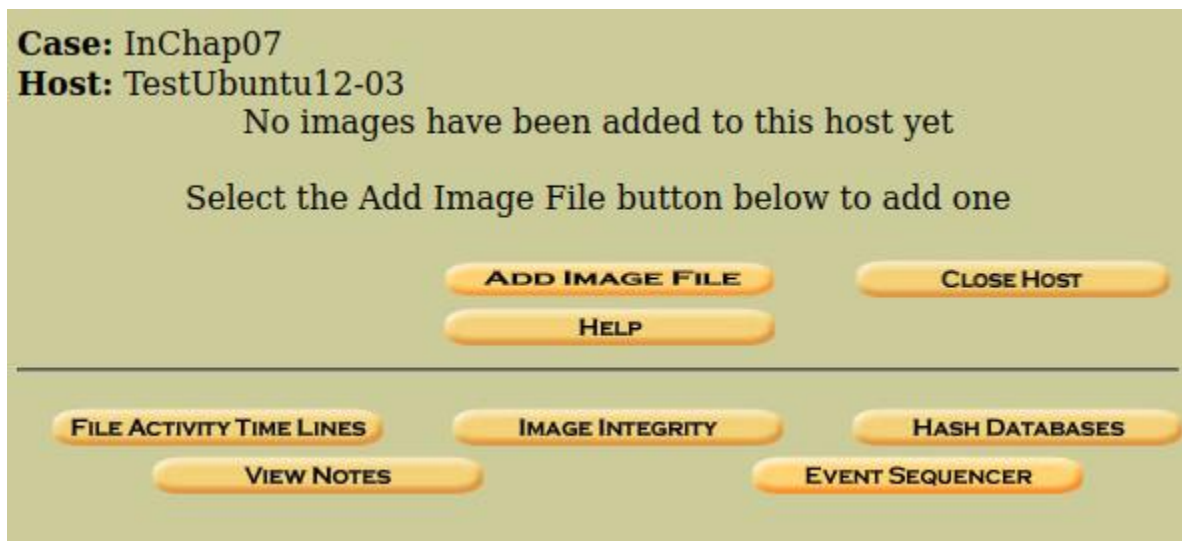
Host Directory (/var/lib/autopsy/InChap07/TestUbuntu12-03/) created

Configuration file (/var/lib/autopsy/InChap07/TestUbuntu12-03/host.aut) created

We must now import an image file for this host

ADD IMAGE

I pressed the add image file to add my subject files.



I entered the full location path of the image files. I selected the partition for the type and move for the import method. Then pressed next.

1. Location
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. Type
Please select if this image file is for a disk or a single partition.

☐ Disk ☒ Partition

3. Import Method
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

☐ Symlink ☐ Copy ☒ Move

NEXT

I was presented with a list of my files. I pressed next to continue.



In the image file details page, I selected "Calculate the hash value for this image" option and then pressed the add button.

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- ☐ Ignore the hash value for this image.
- ☒ Calculate the hash value for this image.
- ☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ext3)

Mount Point:

File System Type:

ADD

CANCEL

HELP

I allowed a few moments for the MD5 hash to calculate on the 1GB image file. The page then loaded the results. I pressed Ok to continue. And the image should show mounted as the file system type ext.

Calculating MD5 (this could take a while)

Current MD5: 26EE697C8D47165383B6F3BD8AE94AAB

Testing partitions

Moving image(s) into evidence locker

Image file added with ID `img1`

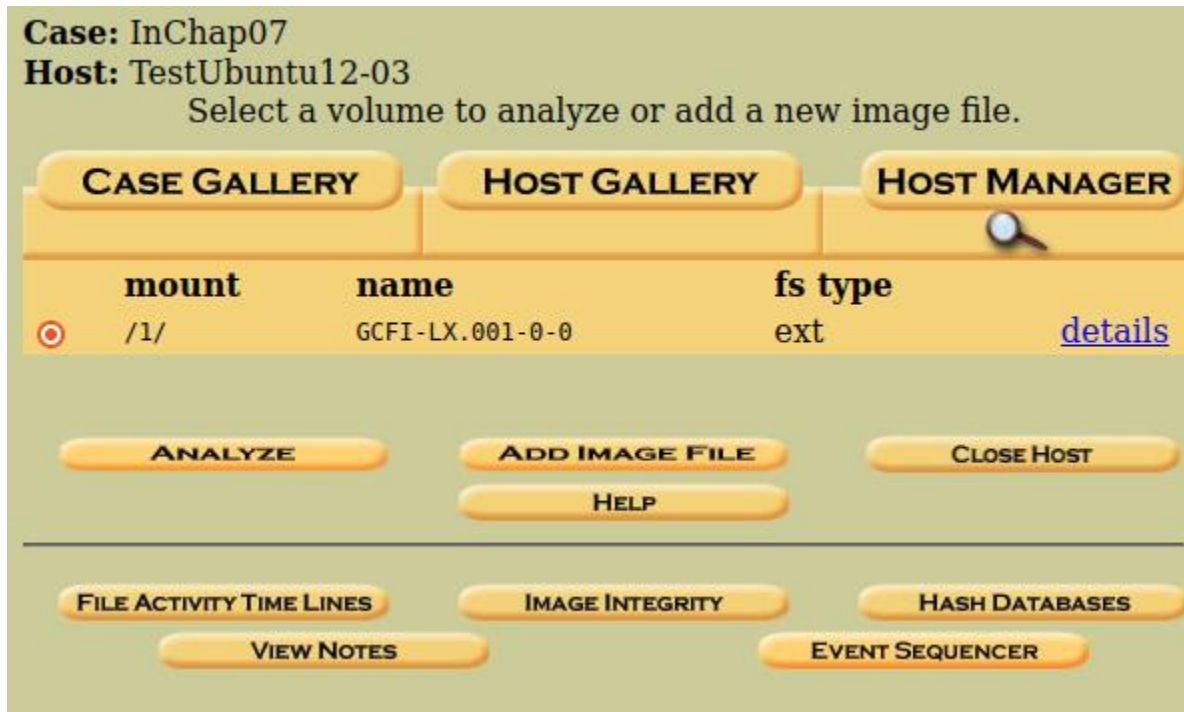
Volume image (0 to 0 - ext - /1/) added with ID `vol1`

OK

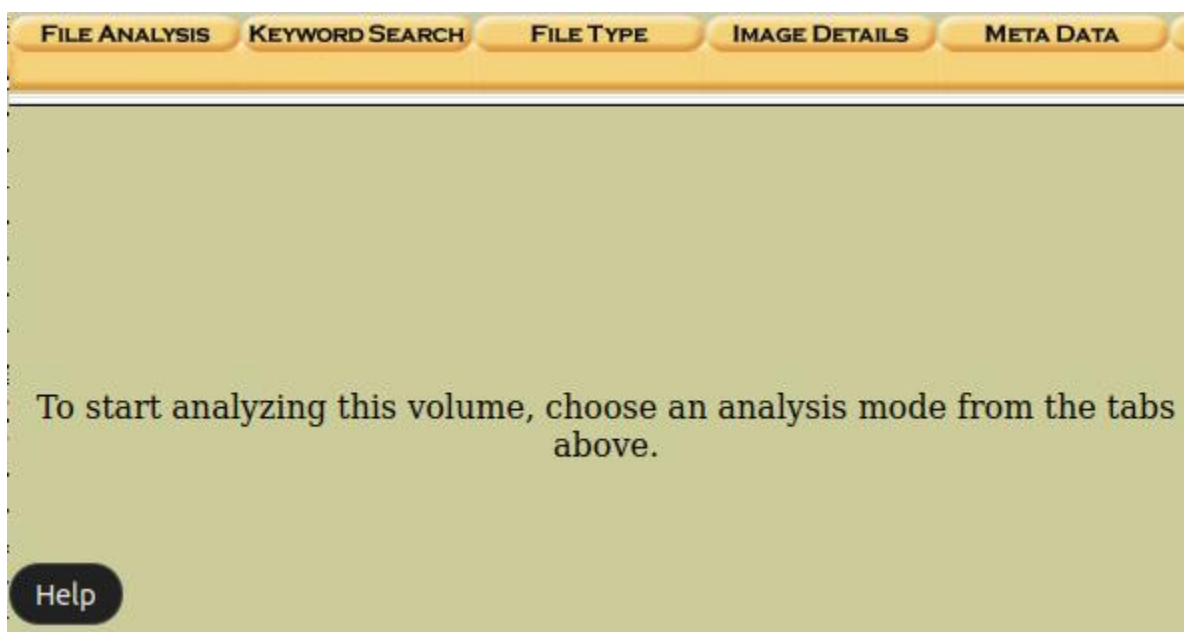
ADD IMAGE

Step 5: Analyze the Image

With the image successfully added to the created case, and while on the “Select a volume to analyze or add a new image file” page, I pressed the analyze button to start the analysis.



I selected the keyword search button from the top menu bar.



I entered the string “martha” into the search field and then clicked search.

The screenshot shows a web application interface for keyword searching. At the top, there is a navigation bar with five tabs: "FILE ANALYSIS", "KEYWORD SEARCH" (which is active and highlighted in orange), "FILE TYPE", "IMAGE DETAILS", and "META DATA". Below the navigation bar, the main heading is "Keyword Search of Allocated and Unallocated Space". Under this heading, there is a prompt "Enter the keyword string or expression to search for:" followed by a text input field containing the word "martha". Below the input field, there are four checkboxes: "ASCII" (checked), "Unicode" (checked), "Case Insensitive" (unchecked), and "grep Regular Expression" (unchecked). A yellow "SEARCH" button is positioned below these checkboxes. Below the "SEARCH" button, there are two yellow buttons: "EXTRACT STRINGS" and "EXTRACT UNALLOCATED". Below these buttons is a blue hyperlink labeled "Regular Expression Cheat Sheet". At the bottom of the form, there is a red "NOTE:" followed by the text "The keyword search runs grep on the image. A list of what will and what will not be found is available [here](#)."

I allowed a few moments for the search to complete. Once it was completed, I observed the summary of the search results. I selected “Link to results” link in the upper left corner of the results.

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

Searching for ASCII:

Done

Saving: Done

77 hits- [link to results](#)

Searching for Unicode: Done

Saving: Done

0 hits

New Search

77 occurrences of martha were found

Search Options:

ASCII

Case Sensitive

I explored the presented ASCII links for some of the occurrences.

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

77 occurrences of martha were found

Search Options:

ASCII

Case Sensitive

← PREVIOUS

NEXT →

EXPORT CONTENTS

ADD NOTE

ASCII ([display](#) - [report](#))

* Hex (display - [report](#))

* ASCII Strings ([display](#) - [report](#))

Hex Contents of Fragment 236019 in GCFI-LX.001-0-0

0	0000000d 00000001 00000052 45c65d85
...	R E.].	
16	00000029 00000004 00000003 00000000	...) ..
...	
32	00000001 00000001 0002af6e 82329a7a
...	n .2.z	
48	8544feb8 4044feb4 c8965765 6c636f6d	.D.. @D..
...	We lcom	
64	6520746f 2045766f 6c757469 6f6e21aa	e to Evo
...	luti on!.	
80	54686520 45766f6c 7574696f 6e205465	The Evol
...	utio n Te	
96	616d203c 65766f6c 7574696f 6e406e6f	am < evol
...	utio n@no	
112	76656c6c 2e636f6d 3ea74576 6f6c7574	vell .com

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@)