

SIT282/SIT703 Computer Forensics and Investigations

Workshop Session 2

In the previous session, you have learned how to use Ubuntu VM with VirtualBox. In this session, you will continue using this virtual machine. Please make sure you have completed session 1 before attempting this one.

Through this session, you will use Linux system commands to perform powerful forensic investigations. By solving the forensic tasks, you will be able to search through disk images and gain accumulative information from your search results.

Learning Objectives

1. Explain the meaning of disk image in relation to digital forensics.
2. Demonstrate that you understand and can use the Linux system command “mount” including option for read-only and “unmount”.
3. Define the two important things to remember when mounting a disk image and relate this to digital forensics.
4. Demonstrate the use of “grep” including options for content-based file search.
5. Explain the meaning of content-based and cluster-based file search.
6. Demonstrate the results of “grep” searches using patterns from the tutorial provided and save the results to a file.
7. Explain the search technique(s) you applied to find a connection between given clues.

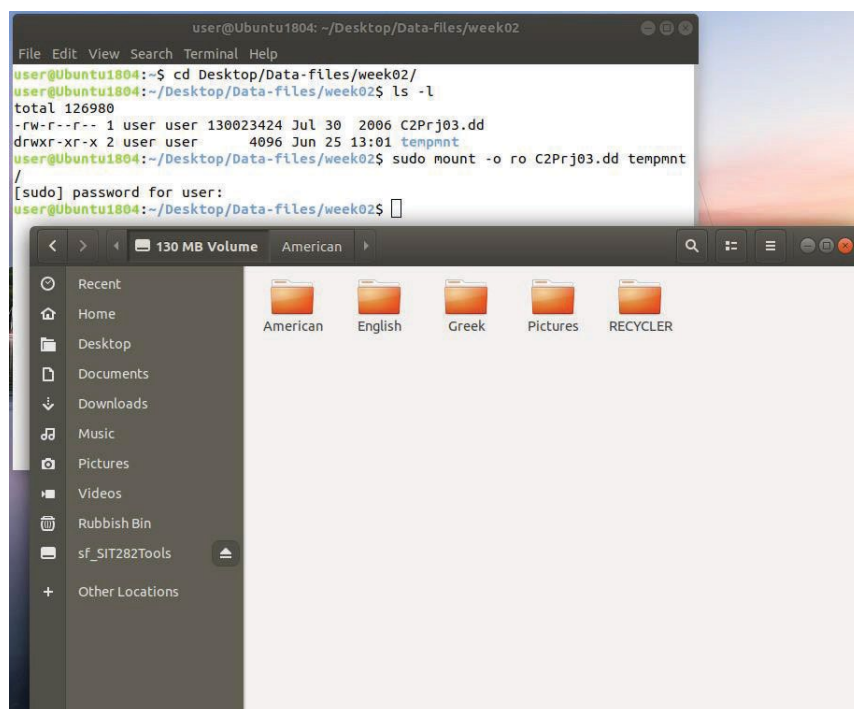
1. Introducing Linux mount

Linux system command “mount” is a powerful tool. It can associate the contents of a disk image with any folder in the system. Once a disk image is mounted, we can browse the image with a simple file browser. There are two important things to remember: 1) always try to mount an image with the **read-only** option, and 2) always remember to use “**sudo**” to mount and umount the image to a folder that you can find.

Launch a “Terminal” in the virtual machine, then change directory to “~/Desktop/Data-files/week02”. You can find a dd image in the folder as well as an empty folder named “tempmnt”. Type command “**sudo mount -o ro C2Prj03.dd tempmnt**” where the option “**-o ro**” is the **read-only** option for mounting the image. Enter the password “**user**”, you will complete the mount process.

```
user@Ubuntu1804: ~/Desktop/Data-files/week02
File Edit View Search Terminal Help
user@Ubuntu1804:~$ cd Desktop/Data-files/week02/
user@Ubuntu1804:~/Desktop/Data-files/week02$ ls -l
total 126980
-rw-r--r-- 1 user user 130023424 Jul 30 2006 C2Prj03.dd
drwxr-xr-x 2 user user 4096 Jun 25 13:01 tempmnt
user@Ubuntu1804:~/Desktop/Data-files/week02$ sudo mount -o ro C2Prj03.dd tempmnt /
[sudo] password for user:
user@Ubuntu1804:~/Desktop/Data-files/week02$
```

Then you can use the file browser tool to navigate through the image. This image contains a few folders with contents and a RECYCLER folder with the information of deleted files.



Now spend 20 minutes or so to explore the contents. You may try to delete or rewrite some of these files and see if it is possible.

2. Search Contents with the tool grep

File search techniques can be broadly classified into two categories: content-based and cluster-based.

Content-based file search involves searching for files based on their content. In this technique, the search query is analyzed and matched against the content of the files. The search results are then ranked based on the similarity of the query and the file content. Content-based search is often used in image search, where the image content is compared to the search query.

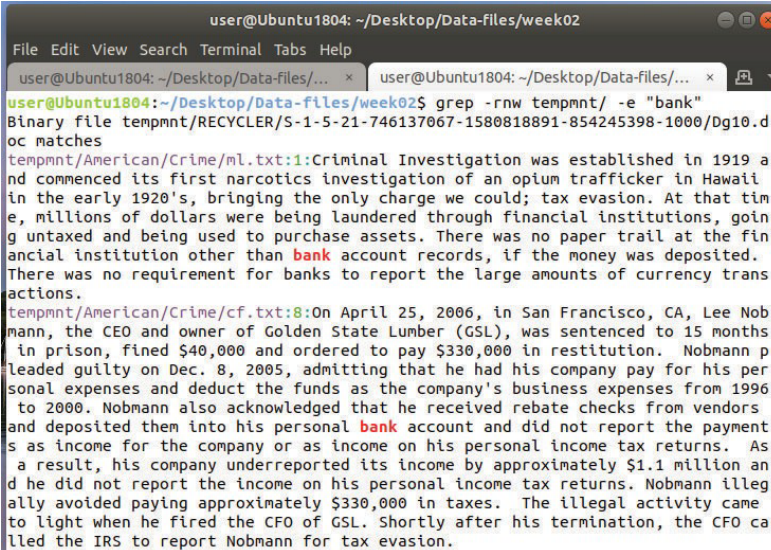
Cluster-based file search, on the other hand, involves grouping similar files into clusters, and then searching for files based on the cluster they belong to. In this technique, the similarity between files is determined by comparing various characteristics such as file type, size, or metadata. The search results are then based on the proximity of the query to the cluster. Cluster-based search is commonly used in web search, where websites are grouped into clusters based on the topics they cover.

In short, content-based file search focuses on the content of the files, while cluster-based file search focuses on grouping similar files together and searching based on the cluster.

Keep the above information in mind, we now use grep to search contents.

Once we have mounted the image to a location, we can perform content-based search through the files. Linux has a powerful search tool named “**grep**”. It supports many powerful functions, but requires some (if not a lot of) practice to master.

Let us use **grep** with a simple example. We can search for a keyword “bank” on the disk image mounted in Section 1. In a Terminal, type in the command “**grep -rnw tempmnt -e “bank”**”, then see the textual results found by the search. (Note: It may take a while to generate the results. For practice purposes, go to American/Crime folder and grep.) Double check if your results are correct. The following screenshot shows the beginning of the results which you will have to scroll upwards to see.



```
user@Ubuntu1804: ~/Desktop/Data-files/week02
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Desktop/Data-files/... x user@Ubuntu1804: ~/Desktop/Data-files/... x
user@Ubuntu1804:~/Desktop/Data-files/week02$ grep -rnw tempmnt/ -e "bank"
Binary file tempmnt/RECYCLER/S-1-5-21-746137067-1580818891-854245398-1000/Dg10.d
oc matches
tempmnt/American/Crime/ml.txt:1:Criminal Investigation was established in 1919 a
nd commenced its first narcotics investigation of an opium trafficker in Hawaii
in the early 1920's, bringing the only charge we could; tax evasion. At that tim
e, millions of dollars were being laundered through financial institutions, goin
g untaxed and being used to purchase assets. There was no paper trail at the fin
ancial institution other than bank account records, if the money was deposited.
There was no requirement for banks to report the large amounts of currency trans
actions.
tempmnt/American/Crime/cf.txt:8:On April 25, 2006, in San Francisco, CA, Lee Nob
mann, the CEO and owner of Golden State Lumber (GSL), was sentenced to 15 months
in prison, fined $40,000 and ordered to pay $330,000 in restitution. Nobmann p
leaded guilty on Dec. 8, 2005, admitting that he had his company pay for his per
sonal expenses and deduct the funds as the company's business expenses from 1996
to 2000. Nobmann also acknowledged that he received rebate checks from vendors
and deposited them into his personal bank account and did not report the payment
s as income for the company or as income on his personal income tax returns. As
a result, his company underreported its income by approximately $1.1 million an
d he did not report the income on his personal income tax returns. Nobmann illeg
ally avoided paying approximately $330,000 in taxes. The illegal activity came
to light when he fired the CFO of GSL. Shortly after his termination, the CFO ca
lled the IRS to report Nobmann for tax evasion.
```

Option “-r” is a recursive option allowing us to search through every file contained within the folders and subfolders;

Option “-n” is the line number which helps us find the original place;

Option “-w” is the whole word match which helps us find the exact matches.

Option “-e “bank” specifies the search pattern as the word “bank”.

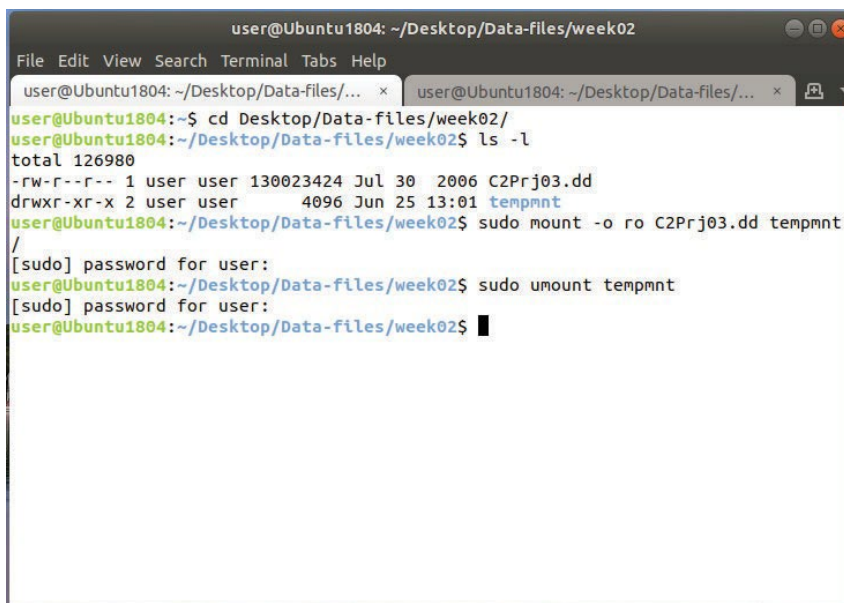
We only used a very simple case to find exact matching keyword. The tool “grep” supports many other patterns including regular expressions. Spend 30 minutes or so to read through the following tutorial:

<https://www.digitalocean.com/community/tutorials/using-grep-regular-expressions-to-search-for-text-patterns-in-linux>. A copy of this tutorial (in pdf) is also available on CloudDeakin for your convenience.

If you wish to save the search results, you may type the following command “**grep -rnw tempmnt -e “bank” > searchresults.txt**”, and then the results will be stored in the file “searchresults.txt”.

3. Introducing the tool umount

The tool “umount” is opposite to the tool “mount”. We need to unmount the disk image once we complete the investigation. Type in the command “**sudo umount tempmnt**”, and then we will no longer see the contents.



```
user@Ubuntu1804: ~/Desktop/Data-files/week02
File Edit View Search Terminal Tabs Help
user@Ubuntu1804: ~/Desktop/Data-files/... x user@Ubuntu1804: ~/Desktop/Data-files/... x
user@Ubuntu1804:~$ cd Desktop/Data-files/week02/
user@Ubuntu1804:~/Desktop/Data-files/week02$ ls -l
total 126980
-rw-r--r-- 1 user user 130023424 Jul 30 2006 C2Prj03.dd
drwxr-xr-x 2 user user 4096 Jun 25 13:01 tempmnt
user@Ubuntu1804:~/Desktop/Data-files/week02$ sudo mount -o ro C2Prj03.dd tempmnt
/
[sudo] password for user:
user@Ubuntu1804:~/Desktop/Data-files/week02$ sudo umount tempmnt
[sudo] password for user:
user@Ubuntu1804:~/Desktop/Data-files/week02$
```