SAT1: 001: LINUX Command Line Essentials

Overview

This lab will show how to manually locate a file in Linux that was discovered as a result of an IDS alert. This lab will also show some basic file analysis. 30 minutes.

Time: 30 Minutes

Learning Objectives

Upon completion of this lab, you should be able to:

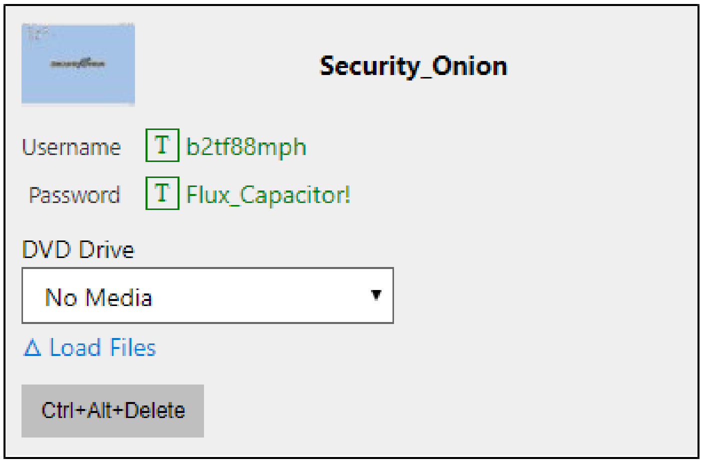
1. Open a Linux Terminal, and locate a file using basic linux commands.
2. Locate helpful information about Linux commands.
3. Create a Directory in the Linux file system.
4. Perform basic file analysis.

What is **Security_Onion**?

Security_Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools.

Log in to the Lab Machine

Select the **Security_Onion** machine on the Machines Tab.



Security_Onion

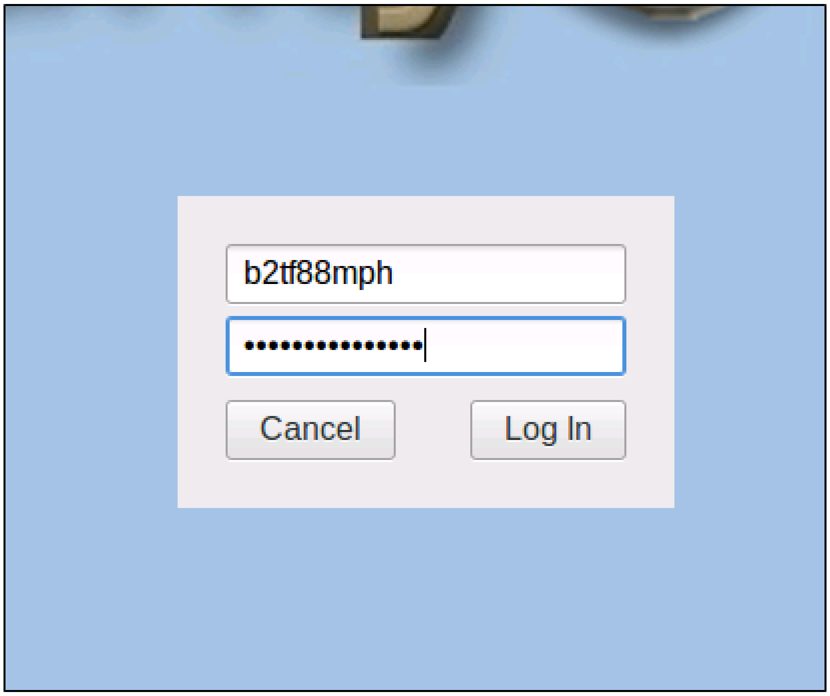
Username T b2tf88mph

Password T Flux_Capacitor!

DVD Drive

No Media ▾

Enter the username and password on the **Security_Onion** machine, and click Log In.



b2tf88mph

•••••••••••••••

Using the LINUX Command Line

LINUX is a family of free and open-source software operating systems based on the Linux kernel, an operating system kernel first released on September 17, 1991 by Linus Torvalds. Linux is typically packaged in a Linux distribution (or distro for short).

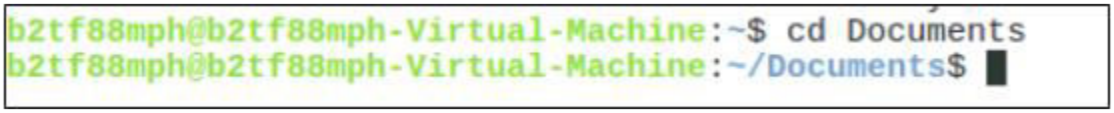
`1.0 Navigation Commands`

1.1 Right click on the Security Onion Desktop, and select Open Terminal.

1.2 Type `pwd` and press Enter. This will show you the current directory you are in.

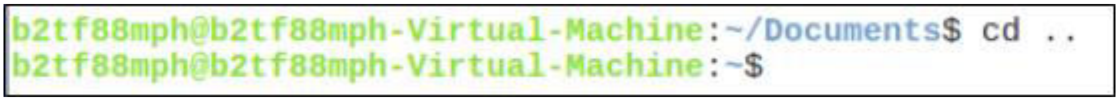
The `cd` command will allow you to change directories.

1.3 Type `cd` and the path to the directory you wish to access. Navigate to the `Documents` folder in the home directory.



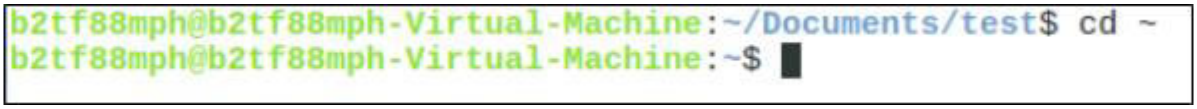
```
b2tf88mph@b2tf88mph-Virtual-Machine:~$ cd Documents
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ █
```

Note: Using the `cd ..` command will allow you to move up one directory level.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ cd ..
b2tf88mph@b2tf88mph-Virtual-Machine:~$
```

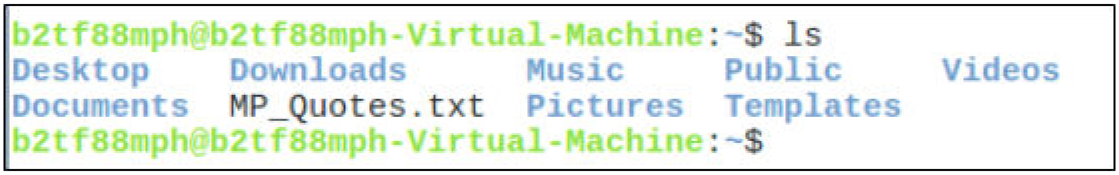
Note: The ~ or tilde command, allows you to move directly to your home directory.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/test$ cd ~
b2tf88mph@b2tf88mph-Virtual-Machine:~$ █
```

`2.0 File Commands`

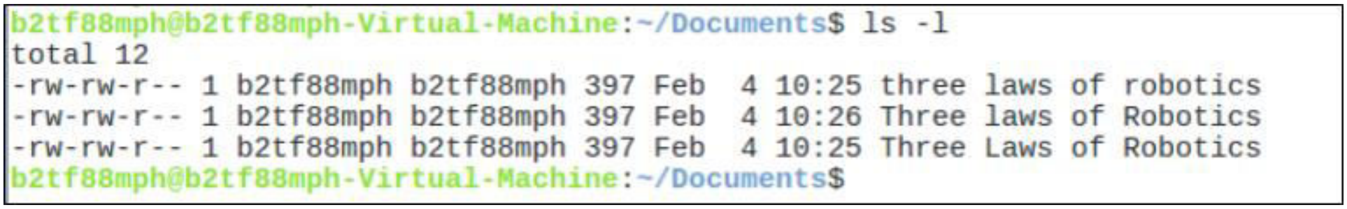
2.1 Type `ls` and press Enter. This will show you a list of all the files and other directories in the current working directory.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~$ ls
Desktop    Downloads      Music     Public     Videos
Documents  MP_Quotes.txt  Pictures  Templates
b2tf88mph@b2tf88mph-Virtual-Machine:~$
```

Using the `ls -l` command will show you a list of all the other files and other directories, as well as details about them.

2.2 Type `ls -l` and press Enter. This provides additional information regarding the files and file permissions.

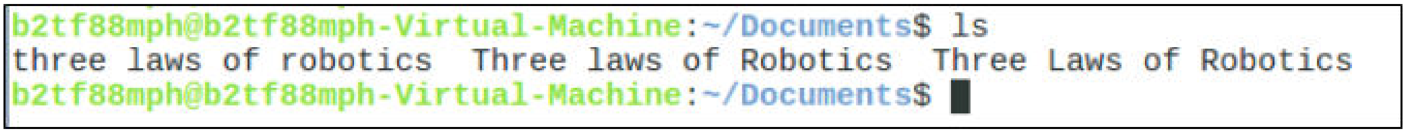


```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls -l
total 12
-rw-rw-r-- 1 b2tf88mph b2tf88mph 397 Feb  4 10:25 three laws of robotics
-rw-rw-r-- 1 b2tf88mph b2tf88mph 397 Feb  4 10:26 Three laws of Robotics
-rw-rw-r-- 1 b2tf88mph b2tf88mph 397 Feb  4 10:25 Three Laws of Robotics
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$
```

NOTE: Linux is an extensionless file system. The commands we are working with will help you analyze files and directories.

2.3 Type `cd Documents` and press Enter. This will change our directory to the `Documents` directory of the current user (b2tf88mph).

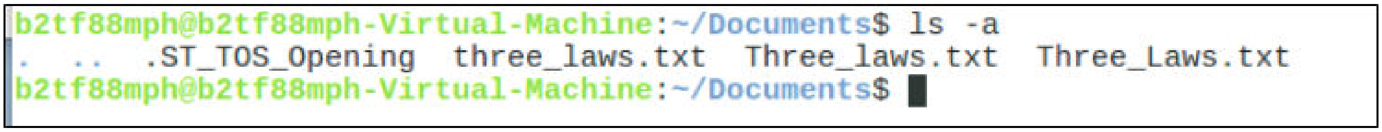
2.4 Type `ls` and press Enter. You should see three different files with similar filenames. Linux is a case-sensitive so adding a capital letter will create a completely different file.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
three laws of robotics  Three laws of Robotics  Three Laws of Robotics
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ █
```

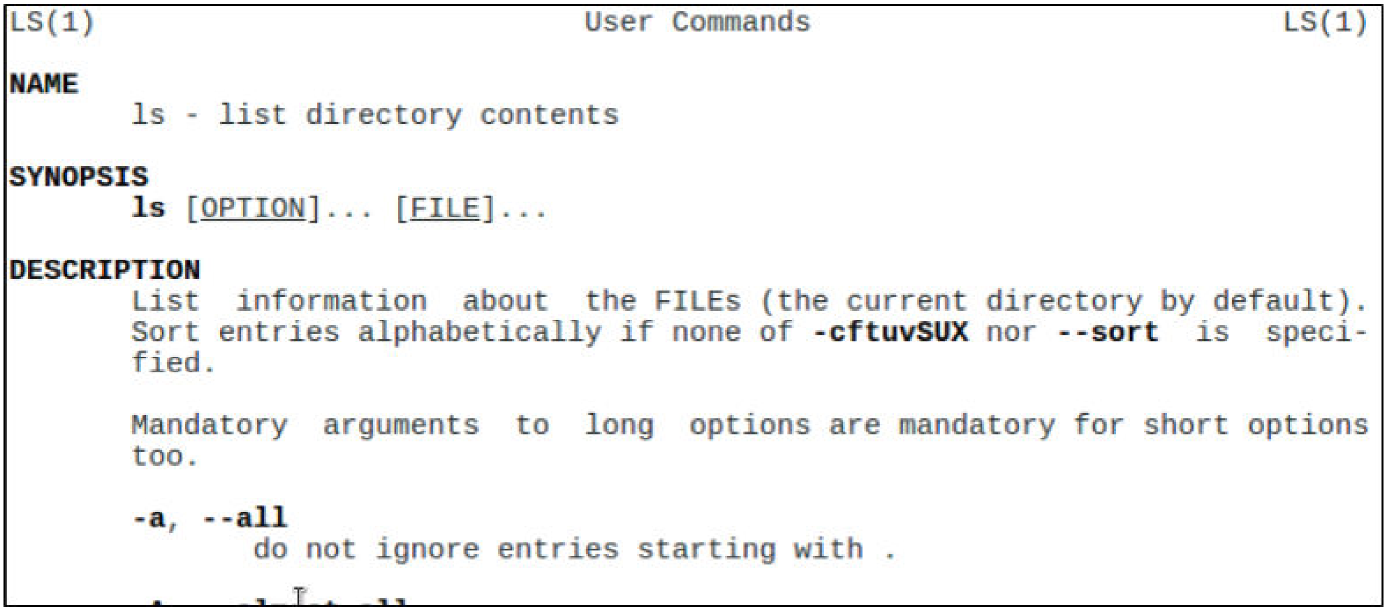
2.5 Type `file three_laws.txt` and press Enter. This will give information regarding the filetype.

2.6 Type `ls -a Documents` and press Enter. This will allow you to see hidden files.



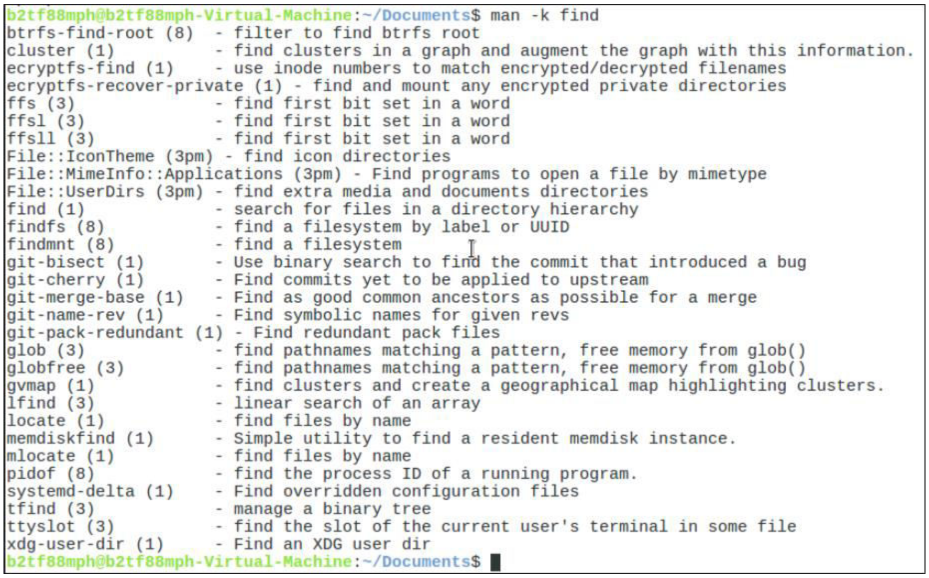
```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls -a
.   ..   .ST_TOS_Opening   three_laws.txt   Three_laws.txt   Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ █
```

2.7 Type `man ls` and press Enter. The manual pages give a description of the application and a list of the associated commands. This can be very helpful if you forget a command option.



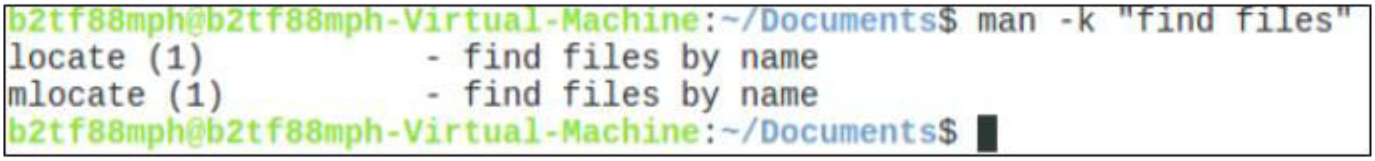
```
LS(1)                            User Commands                           LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about  the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuvSUX nor --sort  is  speci-
       fied.

       Mandatory  arguments  to  long  options are mandatory for short options
       too.

       -a, --all
              do not ignore entries starting with .
```

2.8 Type `man -k find` and press Enter. This gives a fairly long list of commands.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ man -k find
btrfs-find-root (8)  - filter to find btrfs root
cluster (1)          - find clusters in a graph and augment the graph with this information.
ecryptfs-find (1)    - use inode numbers to match encrypted/decrypted filenames
ecryptfs-recover-private (1) - find and mount any encrypted private directories
ffs (3)              - find first bit set in a word
ffsl (3)             - find first bit set in a word
ffsll (3)            - find first bit set in a word
File::IconTheme (3pm) - find icon directories
File::MimeInfo::Applications (3pm) - Find programs to open a file by mimetype
File::UserDirs (3pm) - find extra media and documents directories
find (1)             - search for files in a directory hierarchy
findfs (8)           - find a filesystem by label or UUID
findmnt (8)          - find a filesystem
git-bisect (1)       - Use binary search to find the commit that introduced a bug
git-cherry (1)       - Find commits yet to be applied to upstream
git-merge-base (1)   - Find as good common ancestors as possible for a merge
git-name-rev (1)     - Find symbolic names for given revs
git-pack-redundant (1) - Find redundant pack files
glob (3)             - find pathnames matching a pattern, free memory from glob()
globfree (3)         - find pathnames matching a pattern, free memory from glob()
gvmap (1)            - find clusters and create a geographical map highlighting clusters.
lfind (3)            - linear search of an array
locate (1)           - find files by name
memdiskfind (1)      - Simple utility to find a resident memdisk instance.
mlocate (1)          - find files by name
pidof (8)            - find the process ID of a running program.
systemd-delta (1)    - Find overridden configuration files
tfind (3)            - manage a binary tree
ttyslot (3)          - find the slot of the current user's terminal in some file
xdg-user-dir (1)     - Find an XDG user dir
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ █
```

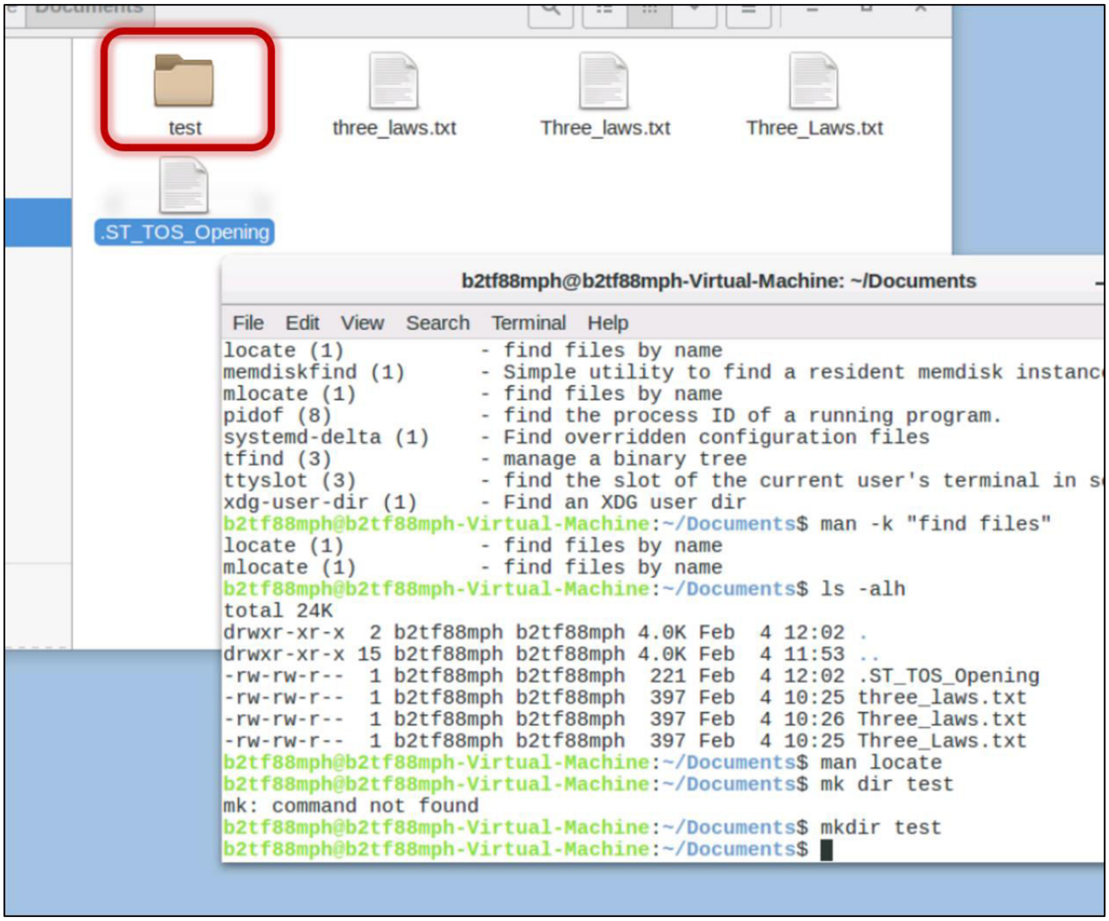
2.9 Type `man -k “find files”`. Now, find the command `locate`.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ man -k "find files"
locate (1)           - find files by name
mlocate (1)          - find files by name
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ 
```

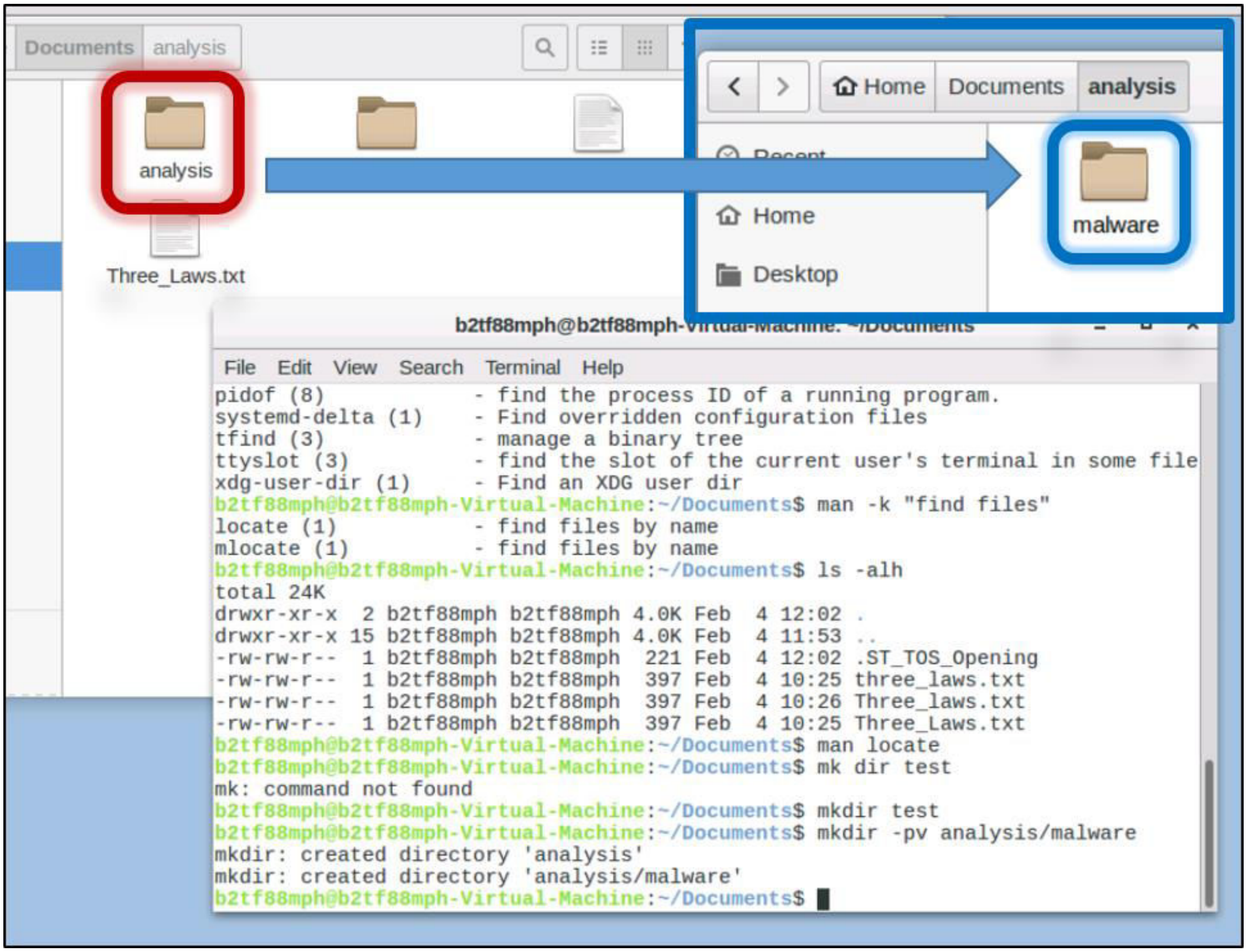
3.0 Directory Commands

3.1 Type `mkdir test` and press Enter. This will create a new directory.



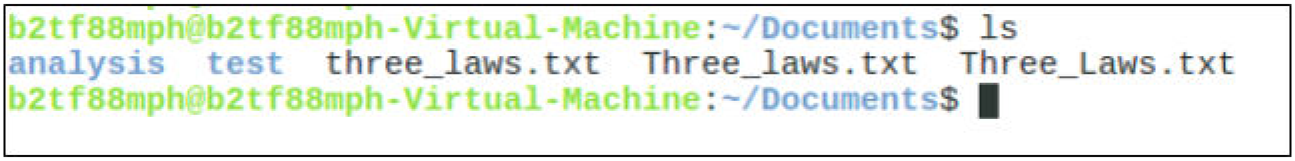
```
locate (1)           - find files by name
memdiskfind (1)      - Simple utility to find a resident memdisk instanc
mlocate (1)          - find files by name
pidof (8)            - find the process ID of a running program.
systemd-delta (1)    - Find overridden configuration files
tfind (3)            - manage a binary tree
ttyslot (3)          - find the slot of the current user's terminal in s
xdg-user-dir (1)     - Find an XDG user dir
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ man -k "find files"
locate (1)           - find files by name
mlocate (1)          - find files by name
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls -alh
total 24K
drwxr-xr-x  2 b2tf88mph b2tf88mph 4.0K Feb  4 12:02 .
drwxr-xr-x 15 b2tf88mph b2tf88mph 4.0K Feb  4 11:53 ..
-rw-rw-r--  1 b2tf88mph b2tf88mph  221 Feb  4 12:02 .ST_TOS_Opening
-rw-rw-r--  1 b2tf88mph b2tf88mph  397 Feb  4 10:25 three_laws.txt
-rw-rw-r--  1 b2tf88mph b2tf88mph  397 Feb  4 10:26 Three_laws.txt
-rw-rw-r--  1 b2tf88mph b2tf88mph  397 Feb  4 10:25 Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ man locate
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ mk dir test
mk: command not found
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ mkdir test
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ 
```

3.2 Type `mkdir -pv analysis/malware` and press Enter. The `-p` option will create parent directories as needed, and the `-v` option gives verbose output from the command.



```
pidof (8)            - find the process ID of a running program.
systemd-delta (1)    - Find overridden configuration files
tfind (3)            - manage a binary tree
ttyslot (3)          - find the slot of the current user's terminal in some file
xdg-user-dir (1)     - Find an XDG user dir
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ man -k "find files"
locate (1)           - find files by name
mlocate (1)          - find files by name
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls -alh
total 24K
drwxr-xr-x  2 b2tf88mph b2tf88mph 4.0K Feb  4 12:02 .
drwxr-xr-x 15 b2tf88mph b2tf88mph 4.0K Feb  4 11:53 ..
-rw-rw-r--  1 b2tf88mph b2tf88mph  221 Feb  4 12:02 .ST_TOS_Opening
-rw-rw-r--  1 b2tf88mph b2tf88mph  397 Feb  4 10:25 three_laws.txt
-rw-rw-r--  1 b2tf88mph b2tf88mph  397 Feb  4 10:26 Three_laws.txt
-rw-rw-r--  1 b2tf88mph b2tf88mph  397 Feb  4 10:25 Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ man locate
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ mk dir test
mk: command not found
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ mkdir test
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ mkdir -pv analysis/malware
mkdir: created directory 'analysis'
mkdir: created directory 'analysis/malware'
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ 
```

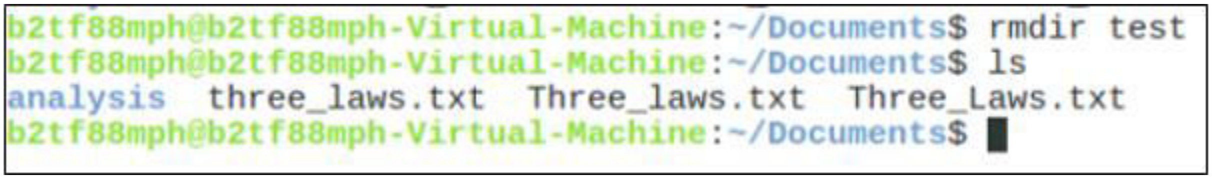
3.3 Type `ls` to see the new directory.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
analysis  test  three_laws.txt  Three_laws.txt  Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ 
```

3.4 Type `rmdir test` and press Enter. This will remove the test directory you created.

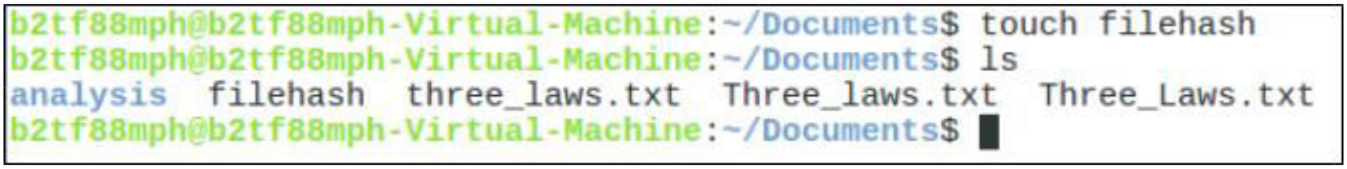
3.5 Type `ls` to see that the directory was removed.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ rmdir test
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
analysis  three_laws.txt  Three_laws.txt  Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ 
```

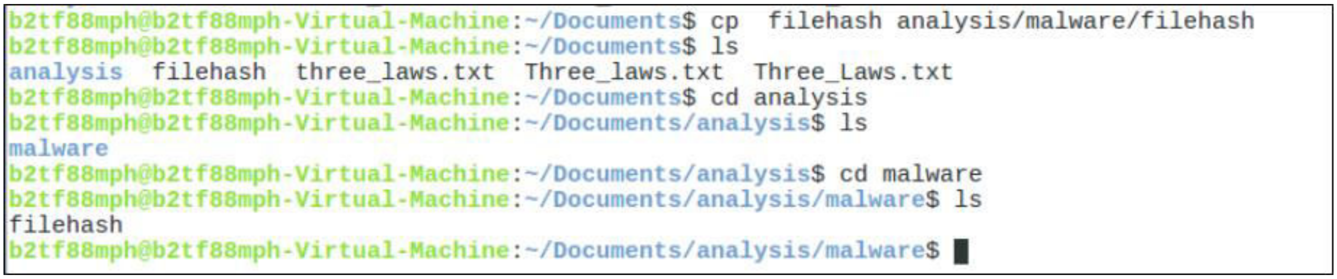
3.6 Type `touch filehash` and press Enter. This will create a new empty file.

3.7 Type `ls` and press Enter to validate the file was created.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ touch filehash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
analysis  filehash  three_laws.txt  Three_laws.txt  Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ █
```

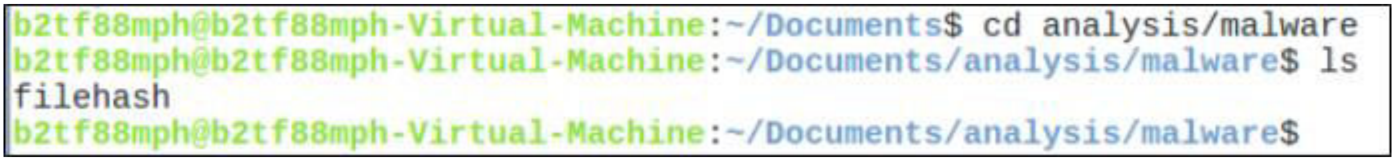
3.8 Type `cp filehash analysis/malware/filehash` and press Enter. This will copy the file to the malware folder.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ cp  filehash analysis/malware/filehash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
analysis  filehash  three_laws.txt  Three_laws.txt  Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ cd analysis
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis$ ls
malware
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis$ cd malware
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ ls
filehash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ █
```

3.9 Type `cd analysis/malware` and press Enter.

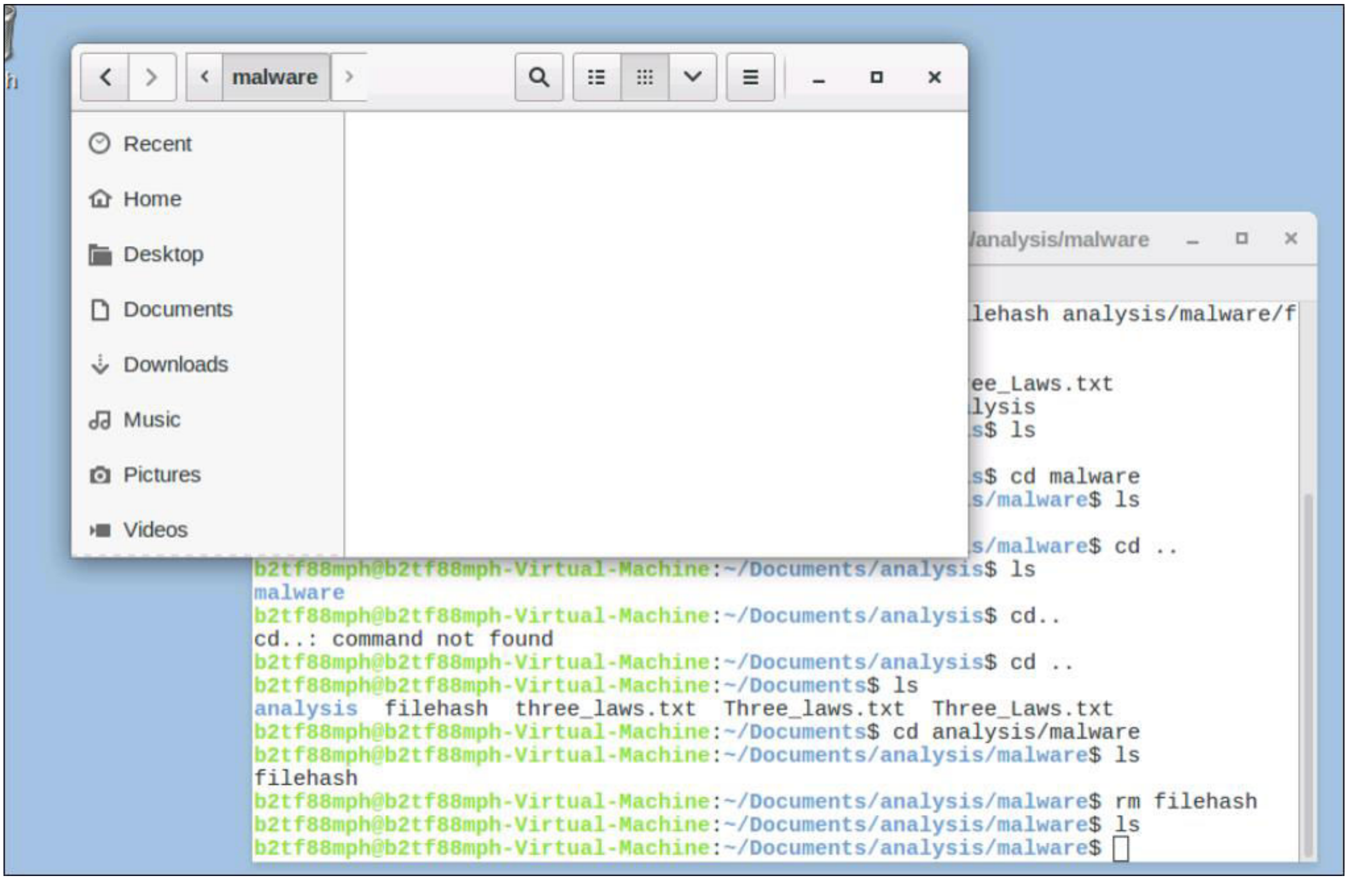
3.10 Type `ls` and press Enter to validate the file was copied.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ cd analysis/malware
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ ls
filehash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$
```

3.11. Type `rm filehash` and press Enter. This will remove the file.

3.12. Type `ls` and press Enter to validate the file was removed.

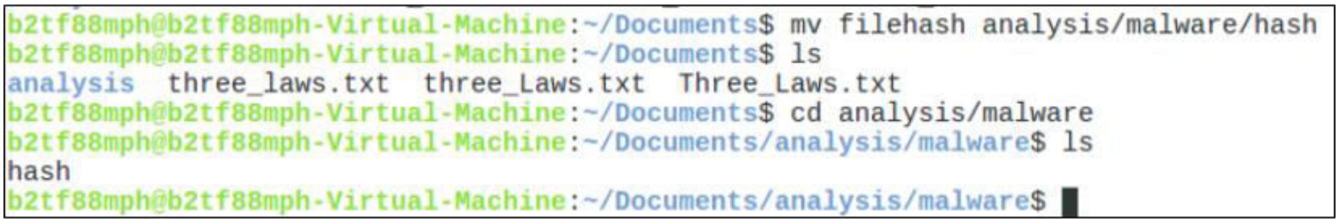


```
lehash analysis/malware/f

ee_Laws.txt
lysis
s$ ls

s$ cd malware
s/malware$ ls

s/malware$ cd ..
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis$ ls
malware
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis$ cd..
cd..: command not found
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis$ cd ..
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
analysis  filehash  three_laws.txt  Three_laws.txt  Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ cd analysis/malware
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ ls
filehash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ rm filehash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ ls
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ 
```

3.13. Type `cd ...` and press Enter. This will take you back up two directories to the original location of the filehash file.

3.14. Type `mv filehash analysis/malware/hash` and press Enter. This will move the file. In addition, you are using the move command to rename the file.

3.15. Type `cd analysis/malware` and press Enter, and type `ls` and press Enter to validate the file was moved.



```
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ mv filehash analysis/malware/hash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ ls
analysis  three_laws.txt  three_Laws.txt  Three_Laws.txt
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents$ cd analysis/malware
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ ls
hash
b2tf88mph@b2tf88mph-Virtual-Machine:~/Documents/analysis/malware$ 
```

Great job, you have completed LAB001!

Thank You, you may now close this module.