Basic Linux Commands Exercise

BitCuratorEdu

Last Updated: January 18, 2022

About This Exercise

Author

Cal Lee

Description

This hands-on exercise is meant to introduce students to basic Linux commands in the BitCurator environment. These slides are excerpted from Cal Lee’s SAA “Advanced Digital Forensics” class. The sample data referenced in these slides is available here: https://github.com/BitCurator/bcc-dfa-sample-data/

Learning object type

Lesson plan/materials

Learning objectives

This learning object might be used in a lesson to satisfy the following learning objectives:

- Practice using tools in the BitCurator Environment.

Command Line Operations

- Opens up many more possibilities, such as:
  - stringing tools together
  - performing batch operations
  - changing parameters from their default values
  - using tools that are only available through the command line (no GUI)

Some Considerations

- Role of pipes – feed output from one process into another process
- Switches – settings that can be applied to a command (e.g. -a, -r)
- Argument – a specific piece of data that is processed by a program (e.g. a variable or fixed value)
- Regular expressions – used to find patterns (more on this later)
- Text created in Windows and Unix, even though they're both ASCII, will encode new lines differently, so you may need to translate usinga tool such as dos2unix or unix2dos.

Some Important Commands and Tasks

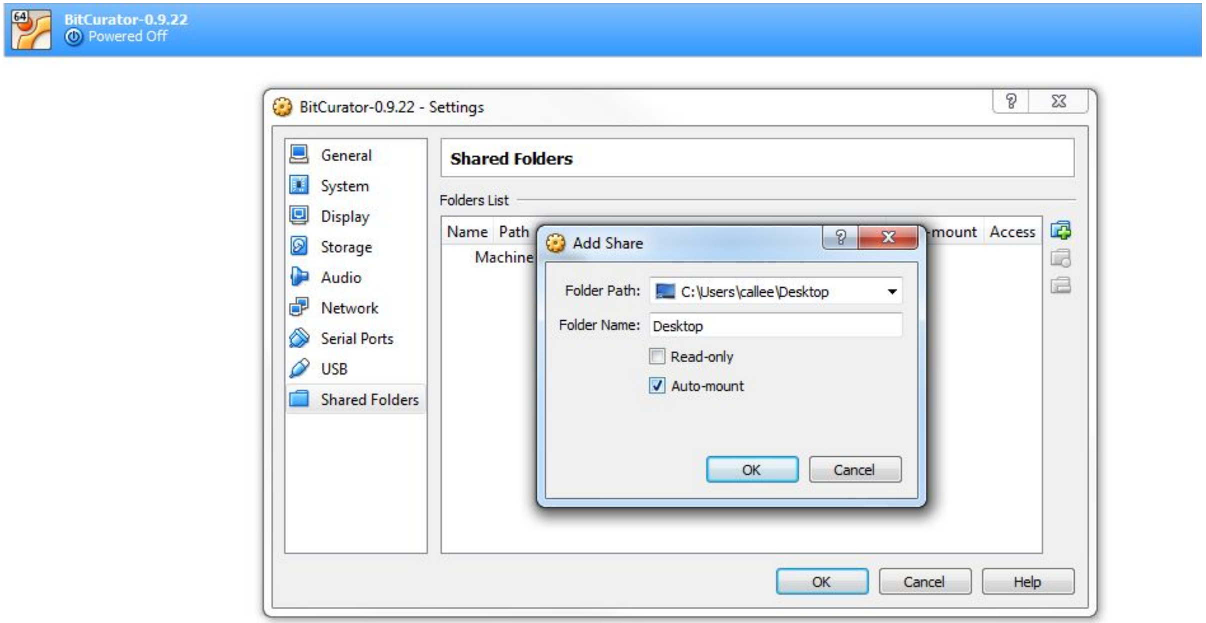
- mkdir – make a directory
- cd – change the directory that you're in ["cd .." goes to the parent of the current directory]
- ls – list contents of a directory
- md5sum – generate cryptographic hashes
- cat – output content of a text file (can be concatenation of contents of two files)
- file – determine file types based on magic numbers
- strings – matches patterns in the text (ASCII) parts of a file (file can be binary)
- diff – compare two files
- hexdump – very basic (non-GUI) hex viewer

General Unix/Linux Tricks

- man – manual page that explains how to run a command or some other technical information (e.g. ascii page)
- control-z – quit currently running program
- clear – clear the screen (hide text from previous commands)
- Up arrow – cycles through previous commands, so you can rerun (or adapt) them
- Tab – hit this key after you've started typing a string that the operating system can fill in for you (e.g. a long file name)

Exercise – Basic Linux Commands

- Copy files.zip to the desktop of your host computer
- If you haven't done this already, add shared folder to BitCurator VM, pointing to the desktop of the host



Folder Path: C:\Users\callee\Desktop

Folder Name: Desktop

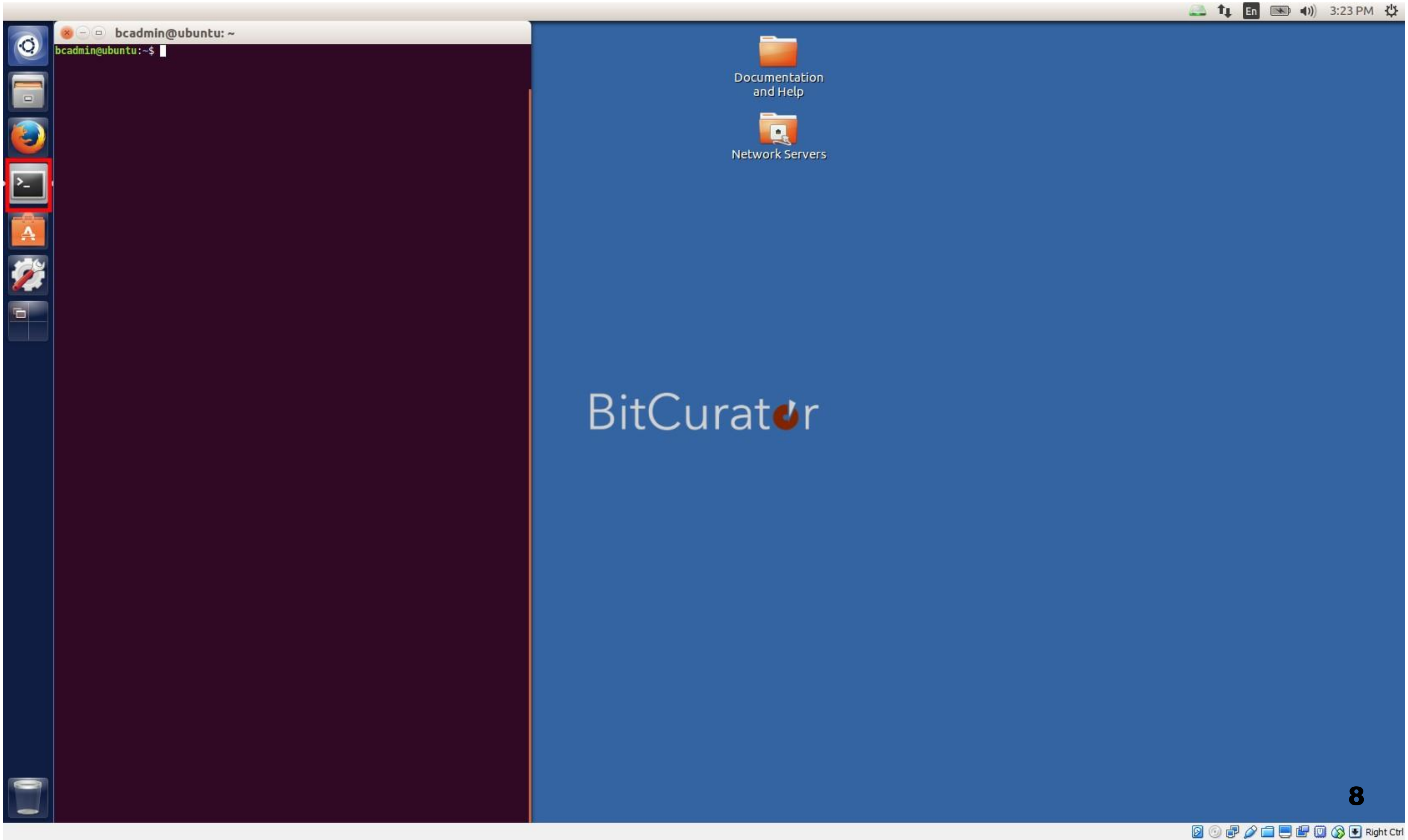
☐ Read-only

☑ Auto-mount

- Move files.zip to the BitCurator VM desktop

Exercise – Basic Linux Commands

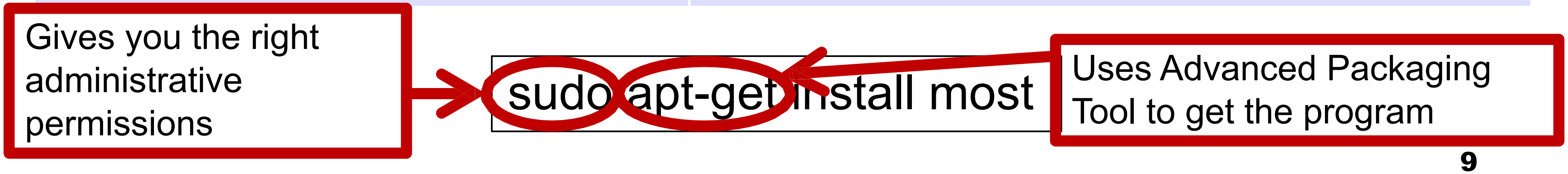
Open a command prompt in the BitCurator environment



```
bcadmin@ubuntu:~$
```

Exercise – Basic Linux Commands

Command	Reason/Explanation
pwd	Show the directory you're currently in
ls	List the contents of the current directory
cd Desktop	Change the current directory to Desktop
ls	List the contents of the current directory
unzip files.zip	Decompress and unpack content of files.zip
ls	List the contents of the current directory
cd files	Change the current directory to files
ls	List the contents of the current directory
md5sum [file name of first file] > firsthash	Create a hash of a file and output it to a text file
less firsthash	Display the content of the output to the screen
Control-z	Stop the "less" program
md5sum [file name of second file] > secondhash	Create a hash of a second file and output it to a text file
cat firsthash secondhash > bothhashes	Combine the context of the two output files
more bothhashes	Display the content of the output to the screen
most bothhashes	Display the content of the output to the screen (follow instructions for adding it), then run this command again



Gives you the right administrative permissions

```
sudo apt-get install most
```

Uses Advanced Packaging Tool to get the program

Exercise – Basic Linux Commands

Command	Reason/Explanation
rm firsthash	Delete (remove) firsthash file
rm secondhash	Delete (remove) secondhash
ls	List the contents of the current directory
hexdump [file name] -C | less	Show hex dump of a given file [-C switch shows the standard view of hex on left and ASCII on right]
Use up and down arrows	Navigate within the hex view of the file’s content
:q	Quit the “less” program

BitCuratorEdu
Advancing the adoption of digital forensics tools and methods in libraries and archives through professional education efforts
EDUCOPIA INSTITUTE Community Cultivators
INSTITUTE of Museum and Library SERVICES

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

The BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.