Edinburgh Napier UNIVERSITY

CSN08101
Digital Forensics
Lecture 2: Essential Linux for Forensics

Module Leader: Dr Gordon Russell
Lecturers: Robert Ludwiniak

Edinburgh Napier UNIVERSITY

Essential Linux for Forensics

You will learn in this lecture:

- Essential file manipulation in Linux
- Command Summary:
  - cp
  - mv
  - cat
  - less
  - more
  - tail
  - head
  - wc
  - chmod
- Concepts Summary
  - Pipe and redirection
  - Basic permissions
  - Filename wildcard expansions

Edinburgh Napier UNIVERSITY

cp

- Duplicates a file.
- Takes 2 parameters:
  - 1. the file being copied
  - 2. the new file being created

$ ls

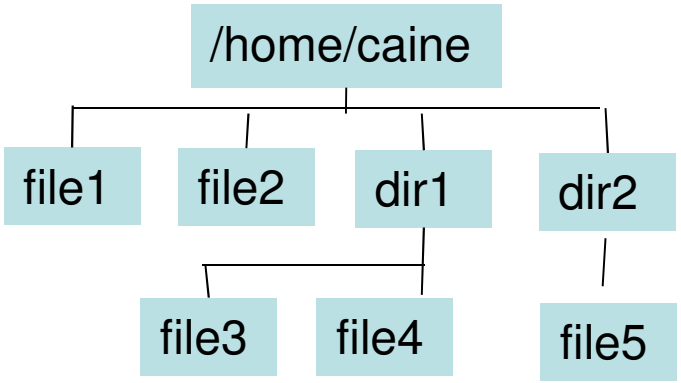
```
file1
```

$ cp file1 file2

$ ls

```
file1        file2
```

Rel/Abs demo



$ cd /home/caine

$ cp dir1/file4 /home/caine/dir2/

- New file is called “file4”

$ cp dir1/file3 /home/caine/dir2/file6

$ cp ../caine/file2 ./dir1

- “.” is the current directory

$ cd dir2

$ cp file5 ..

- “..” is the directory above

Rel/Abs questions

1. Copy file2 into dir2

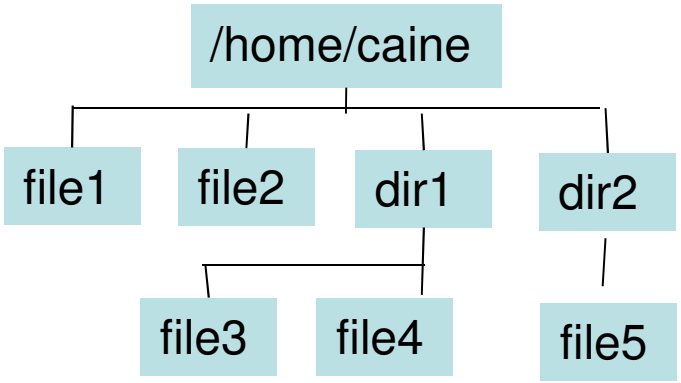
$ cd /home/caine

$ cp file2 ../__???___/__???___/file2

2. Copy file5 into dir1

$ cd dir1

$ cp ?????????/file5 .



Edinburgh Napier UNIVERSITY

mv

- Renames a file.
- Takes 2 parameters:
  - 1. the file being renamed
  - 2. the new filename

$ ls

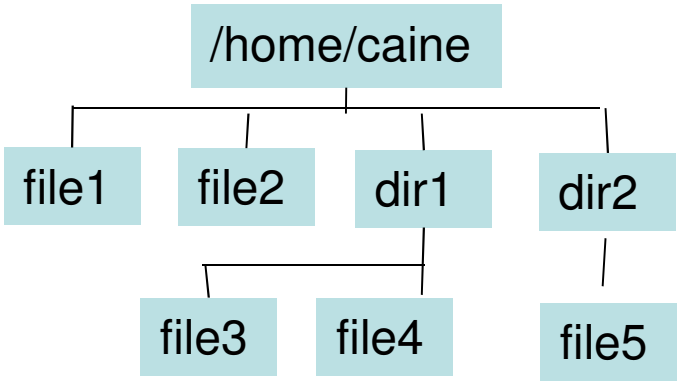
```
file1
```

$ mv file1 file2

$ ls

```
file2
```

Rel/Abs demo



$ cd /home/caine

$ mv dir1/file4 /home/caine/dir2/

- New file is called “file4” but new directory

$ mv dir1/file3 /home/caine/dir2/file6

$ mv ../caine/file2 ./dir1

$ cd dir2

$ mv file5 ..

Rel/Abs questions

1. Rename file2 as filenew

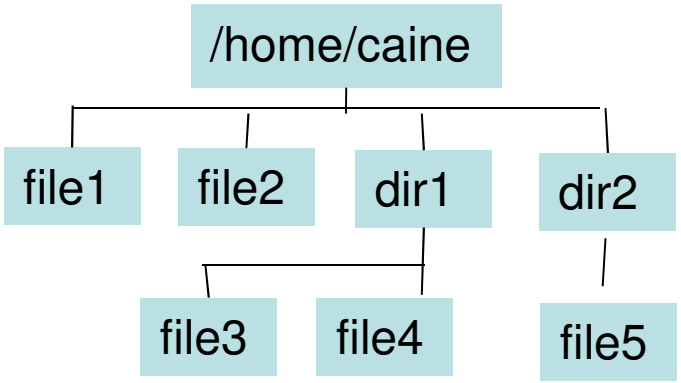
$ cd /home/caine

$ mv file2 dir2/__???___/filenew

2. Rename file4 in dir1 as file10 in /home/caine

$ cd dir2

$ mv ?????????/file4 ????????/file10



cat

- Displays the contents of a file to the screen.

$ cat file1

```
Hello this is the contents of file1
Goodbye
```

$ cat file2

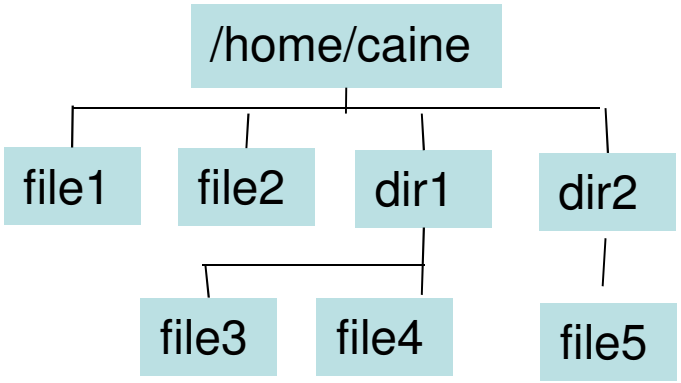
```
Bonjour ici is the contents of file2
Goodbye
```

$ cat file1 file2

```
Hello this is the contents of file1
Goodbye
Bonjour ici is the contents of file2
Goodbye
```

Rel/Abs questions

1. Display the content of file2, file3, and file5 one after the other in a single cat command



$ cd /home/caine

$ cat ??? ??? ???

Edinburgh Napier UNIVERSITY

more

- The user-friendly cat
- Just like “cat” but stops after each full page and says

```
--More--(50%)
```

- Press “spacebar” to continue for another full page
- Press “return/enter” to continue for 1 more line.
- Press “q” to quit out of more before the end of the file.

Edinburgh Napier UNIVERSITY

less

- The user-friendly “more”!
- Just like “more” but you can move backwards.
- Great if you have fat fingers and keep paging past the information you want...
- Same keys as “more”, but also:
  - “Page Up” to go back a page
  - “Page Down” to go on a page
  - Cursor key up arrow to go back 1 line
  - Cursor key down arrow to go on 1 line
- Does not automatically quit at the end. You need to press “q”.

Edinburgh Napier UNIVERSITY

head

- Prints the first “n” lines of a file
  - “n” is 10 by default
  - The first parameter can be “-number”, to give that number of lines from the start of the file
  - Example: you can say “-5” before the name of the file to get the first 5 lines.

$ head -2 file10

```
This is line 1
This is line 2
```

$ head -3 file10

```
This is line 1
This is line 2
This is line 3
```

tail

- Prints the last “n” lines of a file
  - “n” is 10 by default
  - The first parameter can be “-number”, to give that number of lines from the end of the file
  - Example: you can say “-5” before the name of the file to get the last 5 lines.

$ tail -2 file10

```
This is line 99
This is line 100
```

$ tail -3 file10

```
This is line 98
This is line 99
This is line 100
```

Edinburgh Napier UNIVERSITY

wc

- Stands for “word count”.
- By default tells you the number of lines, words, and characters in a file

$ wc /etc/passwd

```
   46   77    2332   /etc/passwd
```

- Useful options include “-l” or “-c” or “-w” to see just the number of lines, characters, or words.

$ wc –l /etc/passwd

```
46     /etc/passwd
```

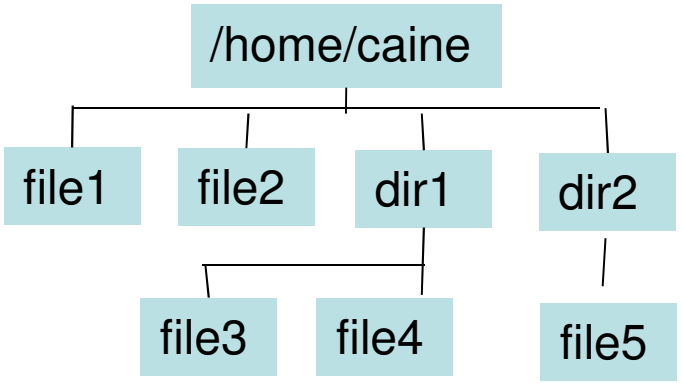
Edinburgh Napier UNIVERSITY

Redirect to a file

- If a command normally prints to the screen you can save this output to a file.
- Simply end the line with “> filename”

```
$ ls -l /etc/hosts
-rw-r--r--. 1 root root 187 Jun  3  2011 /etc/hosts
$ ls –l /etc/hosts > theoutput
$ cat theoutput
-rw-r--r--. 1 root root 187 Jun  3  2011 /etc/hosts
```

Rel/Abs demo



1. Create file10 as the concatenation of file1 and file2.

$ cd /home/caine

$ cat file1 file2 > file10

2. Create file11 as the concatenation of file1, file3 and file5

$ cat file1 dir1/file3 dir2/file5 > file11

Rel/Abs questions

1. Concat file2 and file4 into file55 in /home/caine.

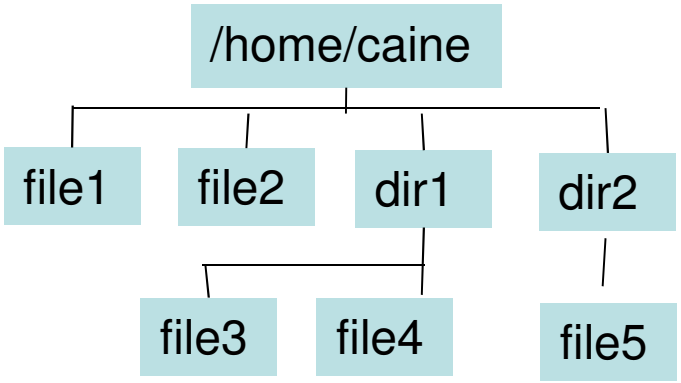
$ cd /home/caine/dir2

$ cat ????/file2 ????/file4 > ?????/file55

2. Duplicate the contents of file1 3 times and save that new file as file9 in dir2.

$ cd

$ cat ???????????? > ????



Edinburgh Napier UNIVERSITY

Redirect to another command

- You can pass the output of one command into the input of the next command in a list of 2 or more commands, all in a single line.

- Example: what is the first file in /etc

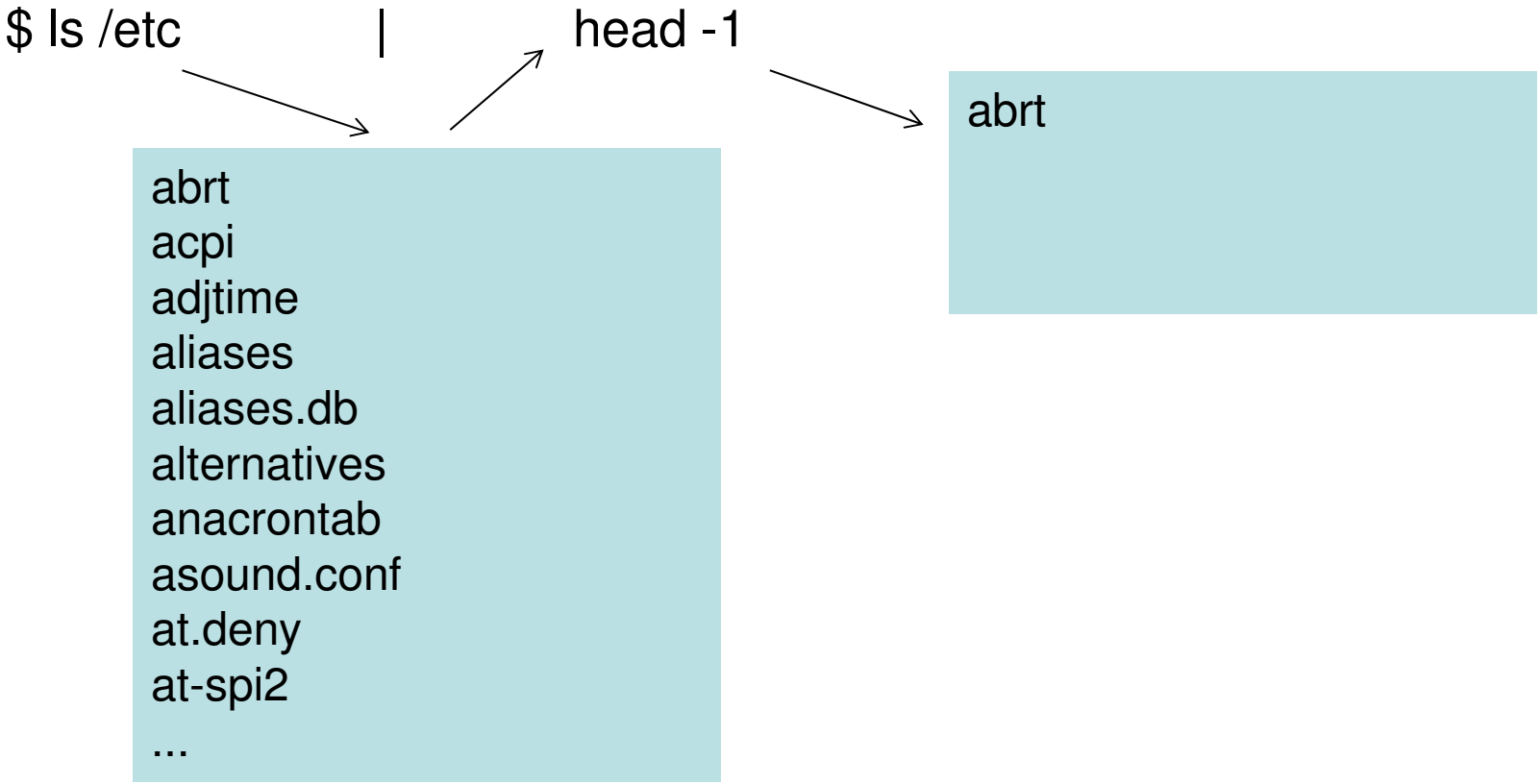
```
$ ls /etc > list
$ head -1 list
abrt
```

- Without the intermediate file “list”:

```
$ ls /etc | head -1
abrt
```

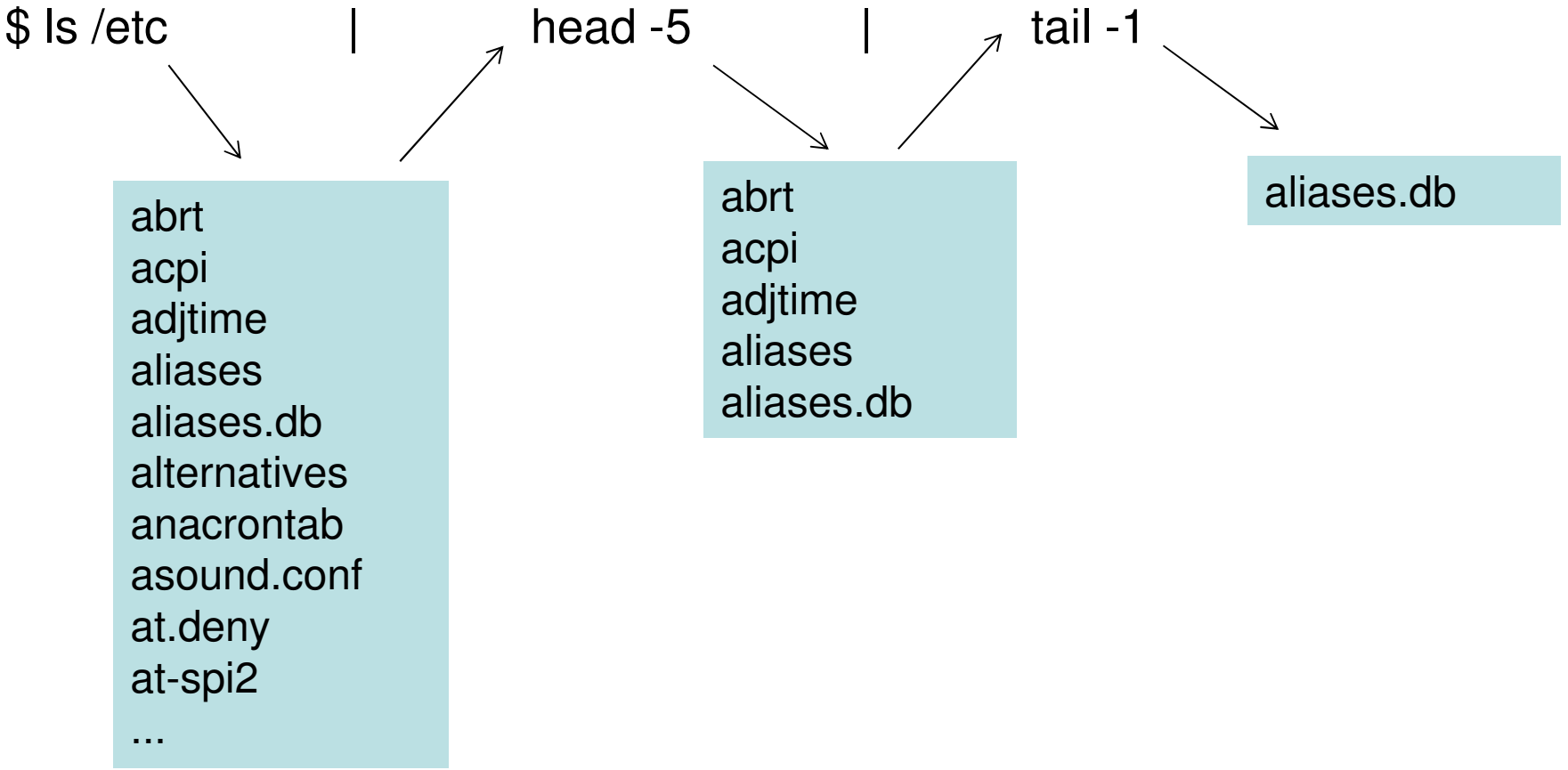
Edinburgh Napier UNIVERSITY

Pipe passes data left to right



Edinburgh Napier UNIVERSITY

Two pipe example: 5th file in /etc



Edinburgh Napier UNIVERSITY

Putting it together

- What is line 3 of the concatination of file1 and file2?

$ cat file1 file2 | head -3 | tail -1

- How many words are on line 7 of /home/caine/mystuff

$ head ???? /home/caine/mystuff | ?????? | ?????

- How many characters are on the third last line of file3?

$ cat file3 | ??????????????????????????????????????

Edinburgh Napier UNIVERSITY

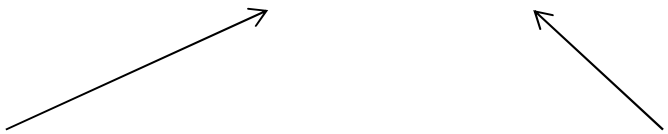
User Permissions

- All modern OSes have a concept of file ownership
- Each file has an owner.
- Often each file also has one or more groups to which is belongs to.
- In Linux, files by default are considered to have 1 owner and 1 group.
- The “ls -l” command allows you to view this easily.

ls –l

$ ls –l file1

```
-rw-r--r--. 1 caine users  1025 Jun  3  2011 file1
```



File Owner: caine

This file has likely been created by the user “caine”

File group: users

The user “caine” likely belongs to the group “users”

Edinburgh Napier UNIVERSITY

Permissions

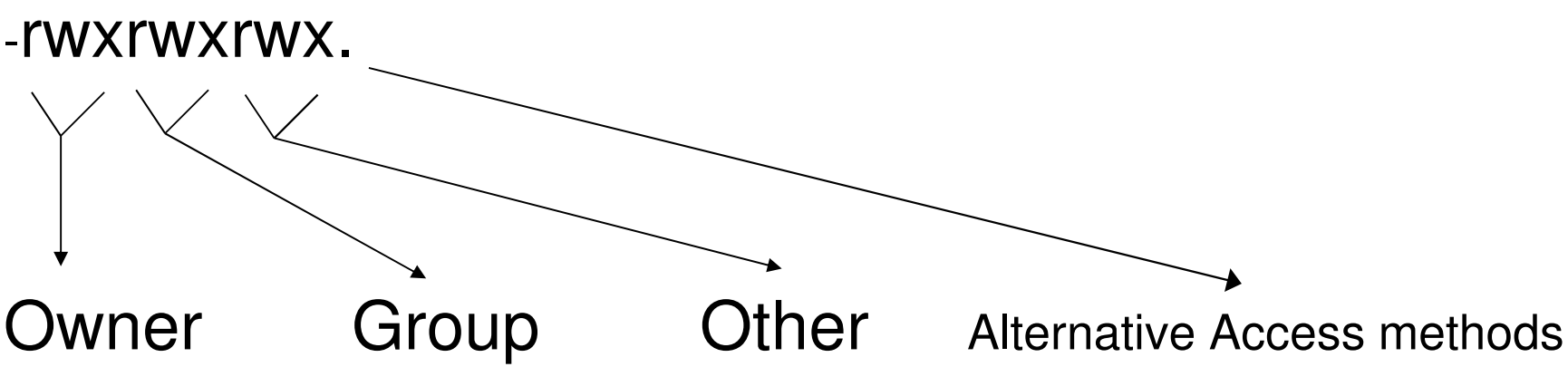
- A file or directory has various permissions and ownerships applied to it.
- Three file permissions:
  - r – read permission
  - w – write permission
  - x – execute permission
- Three permission levels:
  - u – User (the creator of the object)
  - g – Group (a group identifier)
  - o – Other (everyone not in the User or Group specified)

Edinburgh Napier UNIVERSITY

> ls –l /etc/passwd

```
-rw-r--r--.  1 root root 1639 Sep 14 14:38 /etc/passwd
```

- Owned by root, with group root.
- 1639 bytes in size.
- Created on Sep 14th at 14:38.
- 1 link.
- rw by user root
- r by group root
- r by other



- The first character indicates the type of the object.

Edinburgh Napier UNIVERSITY

File types

- - means normal file
- d means directory
- c means a character device (mouse, keyboard)
- b means a block device (ide disk, scsi disk)
- There are more types to discover!

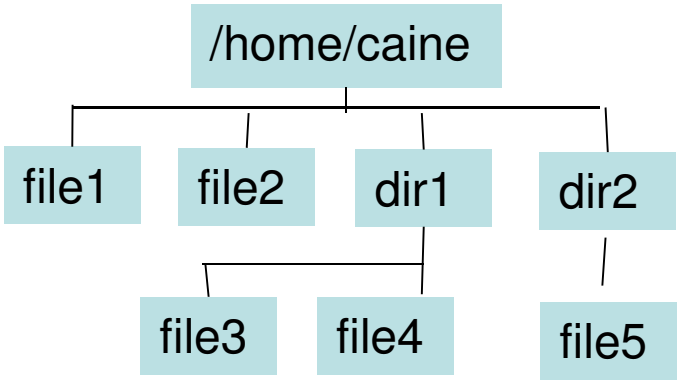
Edinburgh Napier UNIVERSITY

> ls –ld /home

drwxr-xr-x. 2 root root 4096 Jul 27 13:38 /home

- /home is a directory
- Owned by root in group root.
- UID root can do anything, group root can rx
- All others can rx.
- Size is not really useful for directories.

Demo



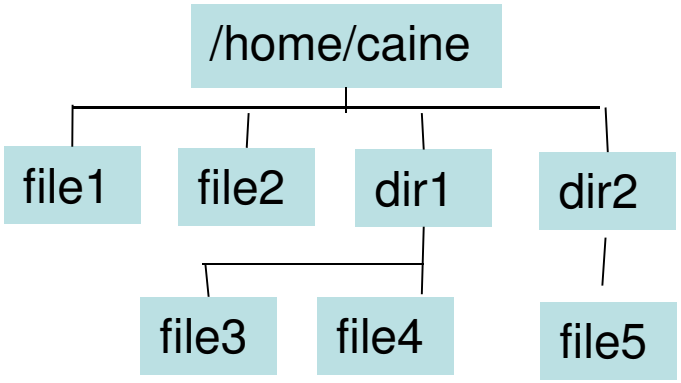
Edinburgh Napier UNIVERSITY

$ ls -l

```
drwxrwxr-x. 2 caine caine 4096 Jan 30 11:52 dir1
drwxr-x--x. 2 caine caine 4096 Jan 30 11:52 dir2
-rw-r--r--. 1 caine caine 187 Jan 30 11:51 file1
-rw-rw-r--. 1 caine caine 374 Jan 30 11:51 file2
```

1. What permission do “others” have on file1 ?
2. What permission does group “caine” have on dir2 ?
3. What permission does group “gordon” have on dir1 ?

Demo 2



Edinburgh Napier UNIVERSITY

$ ls -l

```
-rw-r-xrw-. 1 caine  users 187 Jan 30 11:51 file3
-r--rw-rwx. 1 gordon caine 374 Jan 30 11:51 file4
```

1. What permission does user “gordon”, group “users” have on file3 ?
2. What permission does user “gordon”, group “users” have on file4 ?
3. What permission does user “caine”, group “users” have on file4 ?
4. Can user “gordon” delete file4?

Edinburgh Napier UNIVERSITY

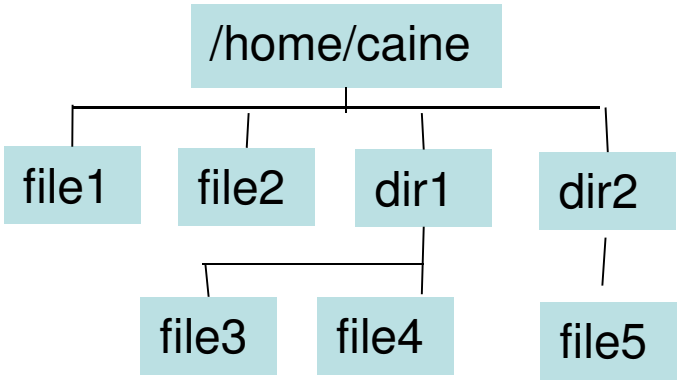
chmod

- This allows the permissions of a file to be controlled.
- It stands for “CHange the MODe” of a file...

- Parameter 1 is the change requested.
- Parameter 2 is the file or directory name being changed

- The change is one or more of “ugo”, then “+-=“, then zero or more of “rwx”.
  - “+” adds permissions to the current set.
  - “-” takes permissions away
  - “=“ does not care what the current permissions are, and deletes them before setting the permissions to that you have specified.

Demo 1



Edinburgh Napier UNIVERSITY

$ ls -l file3

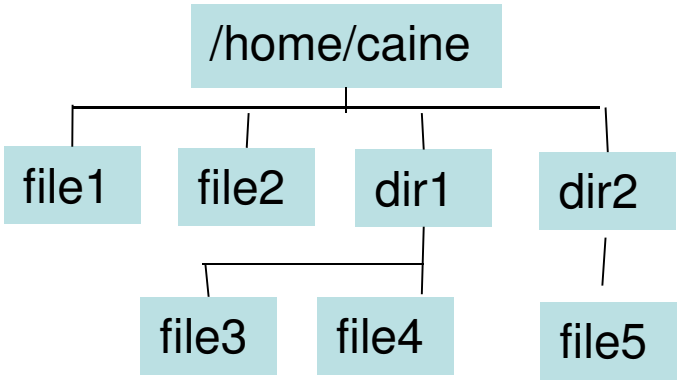
```
-rw-r-xrw-. 1 caine  users 187 Jan 30 11:51 file3
```

$ chmod g+w file3

$ ls -l file3

```
-rw-rwxrw-. 1 caine  users 187 Jan 30 11:51 file3
     ^
```

Demo 2



Edinburgh Napier UNIVERSITY

$ ls -l file3

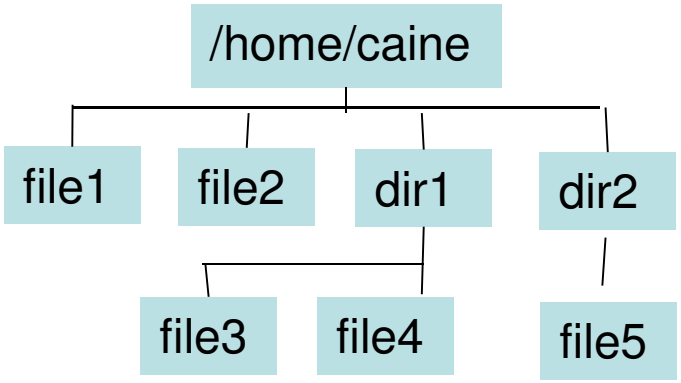
```
-rw-rwxrw-. 1 caine  users 187 Jan 30 11:51 file3
```

$ chmod ugo-w file3

$ ls -l file3

```
-r--r-xr--. 1 caine  users 187 Jan 30 11:51 file3
  ^   ^   ^
```

Demo 3



Edinburgh Napier UNIVERSITY

$ ls -l file3

```
-rwxrw-r--. 1 caine  users 187 Jan 30 11:51 file3
```

1. Give the chmod command for giving file3 execute access for others.
2. Give the chmod command for removing write access to group and owner.
3. What chmod command would remove all permissions for group.

Edinburgh Napier UNIVERSITY

Numeric Notation

- An older way of looking at permissions.
- Still needed for some commands, and a fast way of changing multiple permissions.
- Based on octal, 4 digits long.
- Digit 0 is usually 0, 1 is OWNER, 2 GROUP, 3 OTHER.
- Values:

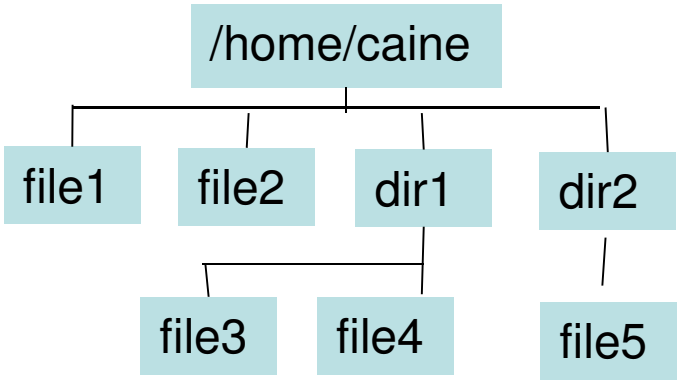
Octal	Binary	Perms	Octal	Binary	Perms
7	111	rwx	3	011	-wx
6	110	rw-	2	010	-w-
5	101	r-x	1	001	--x
4	100	r--	0	000	---

Edinburgh Napier UNIVERSITY

Example

- If User rwx, Group rx, Other rx,
  - Symbolic –rwxr-xr-x
  - Numeric 0755
- If User rwx, Group x, Other none
  - Symbolic –rwx--x---
  - Numeric 0710

Demo 1



Edinburgh Napier UNIVERSITY

$ ls -l file3

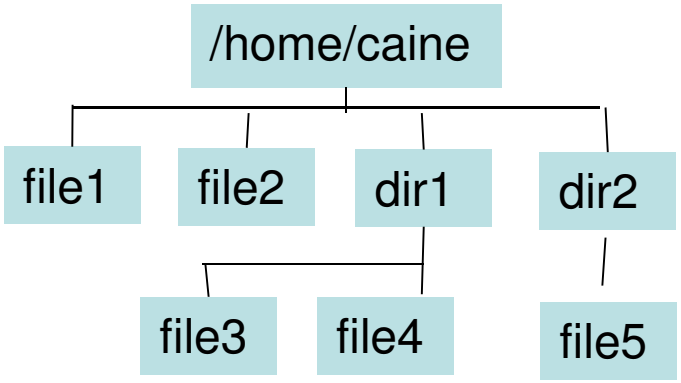
```
-rw-r-xrw-. 1 caine  users 187 Jan 30 11:51 file3
```

$ chmod 676 file3

$ ls -l file3

```
-rw-rwxrw-. 1 caine  users 187 Jan 30 11:51 file3
     ^
```

Demo 2



Edinburgh Napier UNIVERSITY

$ ls -l file3

```
-rw-rwxrw-. 1 caine  users 187 Jan 30 11:51 file3
```

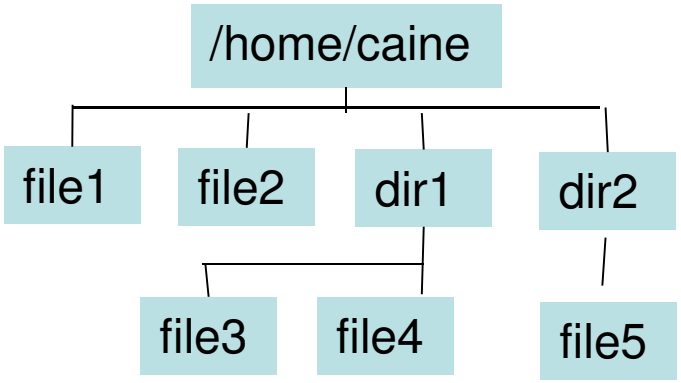
[It was previously chmod ugo-w file3]

$ chmod 454 file3

$ ls -l file3

```
-r--r-xr--. 1 caine  users 187 Jan 30 11:51 file3
  ^   ^   ^
```

Demo 3



Edinburgh Napier UNIVERSITY

$ ls -l file3

```
-rwxrw-r--. 1 caine  users 187 Jan 30 11:51 file3
```

1. Give the chmod command for giving file3 execute access for others.
2. Give the chmod command for removing write access to group and owner.
3. What chmod command would remove all permissions for group.

Edinburgh Napier UNIVERSITY

Executable scripts

- Executable scripts are programs which contain commands.
- These can be executed at the command prompt.
- To do the module you need to create a number of scripts.
  - In each case the script will be supplied to you, but you may have to prepare it.

- If you want to create a file to contain everything from a webpage:
  - Select what you want and then “cut”
  - Use putty to ssh or telnet to your machine
  - If, say, your script is to be called “demo”, go to the right directory and do:
    - $ cat > demo
    - Paste by pressing the right mouse button
    - Once it is all pasted in, press CTRL-D once
  - Now you need to make the script executable
    - $ chmod ogu+x demo
  - Now you can run the script
    - $ ./demo

Edinburgh Napier UNIVERSITY

File Wildcard Expansions

- When a command takes a filename parameter you can specify the exact name.
- But sometimes it is more useful to specify a “wildcard” which allows you to specify a range of filenames.
- For example, you may want to:
  - Copy all files which end “.doc”.
  - Delete all files which end “.deleteme”
  - See how many lines in total are in all the files “evidence01.dat” to “evidence99.dat”.
- When you use this to describe filenames, it is called filename expansion, or globbing, or filename wildcards.
- Do not confuse this with regular expressions, which we will cover in a later lecture. They are not interchangable.

Edinburgh Napier UNIVERSITY

Wildcards

- Parameters which match filenames don't have to be complete. You can pattern match with the characters "?" for a single character and "*" for a number of characters.

$ ls

```
aaa   aab   abb
```

$ ls aa?

```
aaa   aab
```

$ ls a*

```
aaa   aab   abb
```

Edinburgh Napier UNIVERSITY

Wildcard [set]

- You can pattern match with a set of characters. For instance, you want files which end with a or b.

$ ls

```
aaa  aab  aac zzb zzc
```

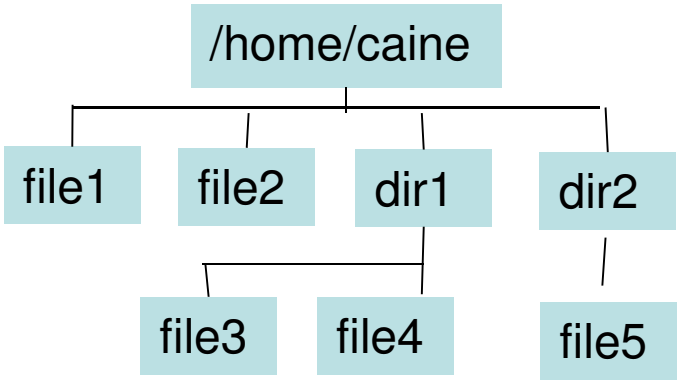
$ ls aa[ab]

```
aaa  aab
```

$ ls *[ab]

```
aaa  aab  zzb
```

Example 1



Edinburgh Napier UNIVERSITY

$ cd /home/caine

$ ls f*

```
file1        file2
```

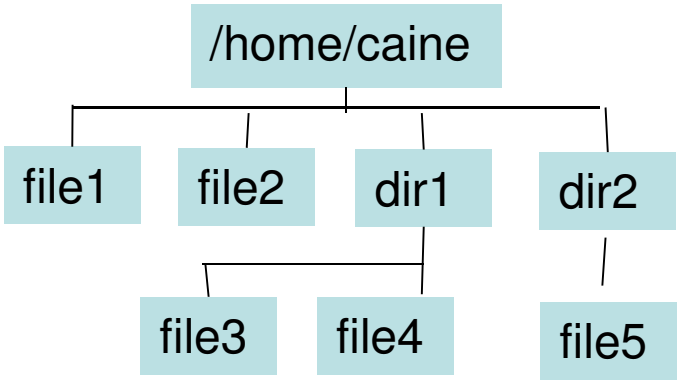
$ ls *i*

```
file1  file2

dir1:
file3  file4

dir2:
file5
```

Example 2



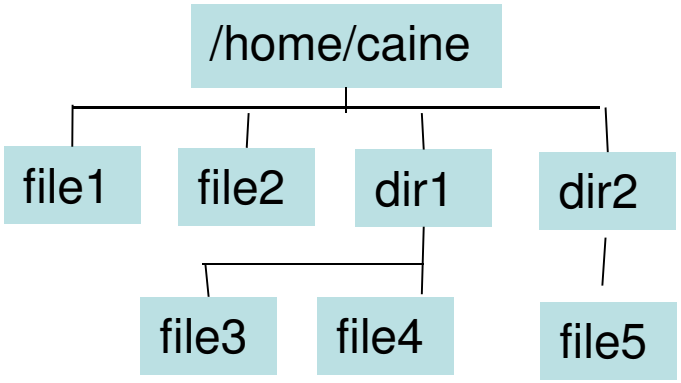
Edinburgh Napier UNIVERSITY

- The “ls” command always wants to show you the contents of specified directories. This can be annoying.
- To disable this behaviour use “-d”.

$ ls -d *i*

```
dir1  dir2  file1  file2
```

Example 3



Edinburgh Napier UNIVERSITY

$ cd /home/caine

1. How many files in the current directory have the number 1 in them?
   - Hint: the “ls” command senses it is in a pipe, and outputs each file on a seperate line.

$ ls ??????? | wc ?????

2

2. In alphanumeric order, what is the second file in /home/caine which ends in the character “2” ?

$ ls ???????? | ?????????????? | ??????????????

Edinburgh Napier UNIVERSITY

Assessment: Short-Answer Examples

- The short answer class test has no past papers yet (as this is a new module for this year).
- This section contains example questions which are of the same style as you might expect in the actual past paper.
- Obviously it is likely that the actual questions shown here are not the ACTUAL questions which will appear in the exam!
- Remember this short answer exam is CLOSED BOOK. You are not permitted to use the internet or access your notes during the exam.

Edinburgh Napier UNIVERSITY

Q1

- There are 3 files in the current directory, “myfile1”, “myfile2”, and “myfile3”. Produce a 1 line command which displays the number of characters which can be found in the last 20 lines of the concatenation of all three files in alphanumeric order.

Insert answer here:

Edinburgh Napier UNIVERSITY

Q2

- How many characters make up the third-last filename shown in a directory listing of the current directory? Your answer should be in the form of a single statement.

Insert answer here:

Edinburgh Napier UNIVERSITY

Q3

- Produce a filename expansion which finds all the files which start with the name “test” and end with the string “data”, and where the data between “test” and “data” takes the form of a two-digit number (i.e. 01, 55, 99, etc). The expansion should not match any other possible filenames.

Insert answer here:

Edinburgh Napier UNIVERSITY

Q4

- A file currently has the numeric permissions 753. What would the resulting numeric permissions be if group was set to read and write only and the owner's permissions had execute removed?

Insert answer here:

Edinburgh Napier UNIVERSITY

Q5

- Consider the following command:

$ ls -l file3

```
-rw-r-xrw-. 1 caine  users 187 Jan 30 11:51 file3
```

- What chmod command, using the symbolic notation, would allow user "gordon" in group "forensics" to run this file as a script?

Insert answer here: