Edinburgh Napier UNIVERSITY

CSN08101
Digital Forensics
Lecture 5: Data management and Autopsy

Module Leader: Dr Gordon Russell
Lecturers: Robert Ludwiniak

Edinburgh Napier UNIVERSITY

Data Management for Forensics

You will learn in this lecture:

- Command Summary:
  - sort
  - xxd
  - echo

- This week is all about:
  - Reading and Writing bytes from binary files
  - sorting
  - Running autopsy

Edinburgh Napier UNIVERSITY

sort

- The “sort” command allows you to take files or data from a pipe and process the data a line at a time using a sorting algorithm.

- In the examples we will use a data file “me.txt”.

$ cat me.txt

```
alpha 20
delta 140
echo 9
beta 15
```

Edinburgh Napier UNIVERSITY

Simple sort

$ cat me.txt

```
alpha 20
delta 140
echo 9
beta 15
```

$ cat me.txt | sort

```
alpha 20
beta 15
delta 140
echo 9
```

Column sort

- You can specify the column to sort using “-k” followed by the start and end column. We will use 1 column keys, so start and end column is always the same. This is an alphanumeric sort.

$ cat me.txt

```
alpha 20
delta 140
echo 9
beta 15
```

$ cat me.txt | sort –k 2,2

```
delta 140
beta 15
alpha 20
echo 9
```

Alphanumeric

- Alphanumeric sort is ASCII ordering.
- If you sort a number then the first character of the number is used, and other characters only considered when two rows have the same first character.

$ cat me.txt | sort –k 2,2

```
delta 140
beta 15
alpha 20
echo 9
```

Numeric sort

- If you are sorting numbers and you want them sorted in numeric order then you must specify this.
- To do numeric sort put an “n” after the start and end column numbers, so “-k 2,2” becomes “-k 2n,2n”

$ cat me.txt | sort –k 2n,2n

```
echo 9
beta 15
alpha 20
delta 140
```

Edinburgh Napier UNIVERSITY

Delimiter

- It is assumed that each column is separated by whitespace.
- If your file is separated by a different character this must be specified using “-t”, followed with the delimiter in quotes with no spaces.

$ cat me2.txt

```
alpha,20
delta,140
echo,9
echo,9
beta,15
```

Delimiter

- So a comma between the columns is specified using:

  -t”,”

$ cat me2.txt | sort –t”,” –k 2n,2n

```
echo,9
echo,9
beta,15
alpha,20
delta,140
```

Uniqueness

Edinburgh Napier UNIVERSITY

- Finally, if two rows are the same then the rows are kept by default.
- Sometimes you want to remove duplicates.
- Use “-u” for unique...

$ cat me2.txt | sort –t”,” –k 2n,2n

```
echo,9
echo,9
beta,15
alpha,20
delta, 140
```

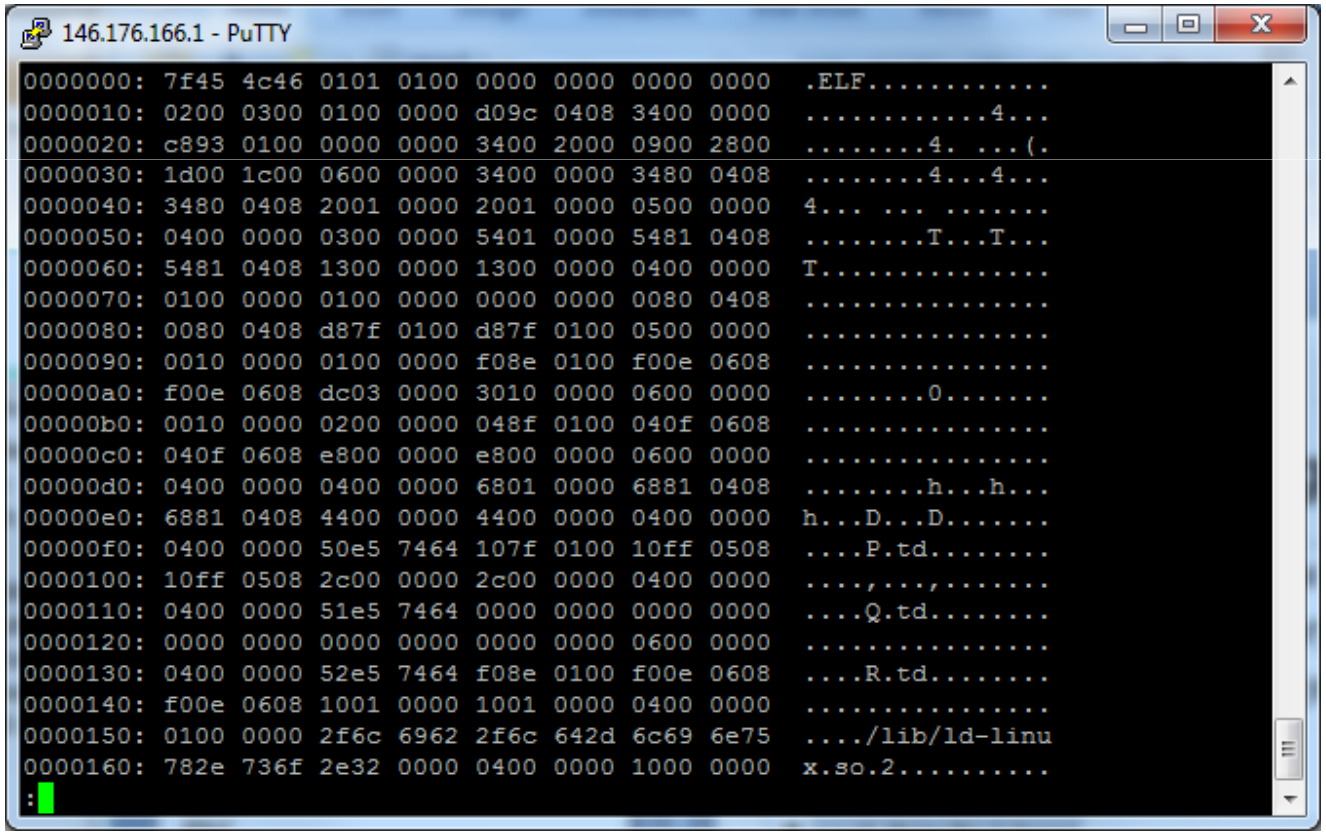
$ cat me2.txt | sort –u –t”,” –k 2n,2n

```
echo,9
beta,15
alpha,20
delta,140
```

Binary file viewing

- Sometimes you want to view the contents of a binary file.
- The normal method for binary viewing is to view it in hexadecimal.
- The “xxd” command allows you to do this, and will display a whole file in hex.

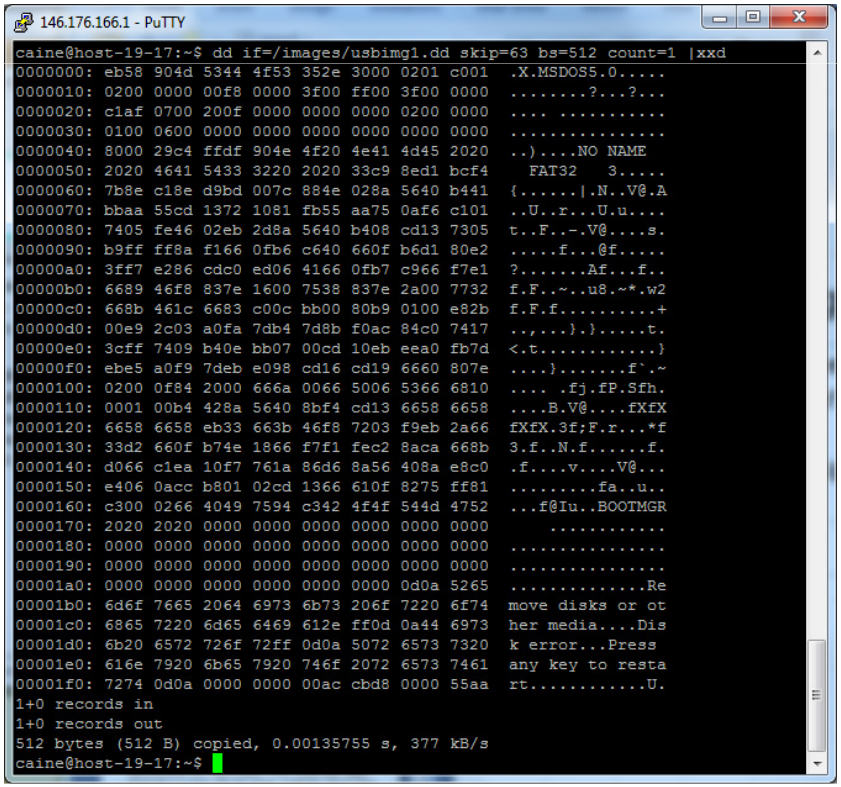
$ xxd /bin/ls | less



Binary file viewing

- If you just want to view some of a file use dd to select what you want.
- For instance, view block 63 of /images/usbimg1.dd

$ dd if=/images/usbimg1.dd skip=63 bs=512 count=1 | xxd



Edinburgh Napier UNIVERSITY

Binary file writing

- If you want to change a byte in a binary file you could use a complicated binary editor.
- However, a simple command line can often get you the same result using dd.
- To generate binary data in a pipe we will use the echo command.
  - Use “-n” to display printing a newline character at the end
  - Use “-e” to allow us to write escape sequences
  - Use “\xCC” where CC is the hex of the binary data to produce.
- For instance, to produce the binary code 0x65 (which in ASCII is the lowercase “e” character) just do:

$ echo –ne “\x65”

Binary file writing

- Echo produces the data

$ echo –ne “\x65”

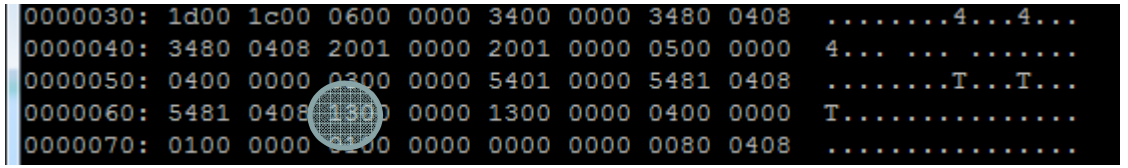
- Use dd in a pipe to write the byte in question.
  - Use a blocksize of 1 byte
  - Use a count of 1
  - Seek to the byte you are changing
  - Remember conv=notrunc to avoid deleting data
- For instance, set byte at offset100 of test.dat to 0xf5

$ echo –ne “\xf5” | dd of=test.dat count=1 bs=1 seek=100 conv=notrunc

Example

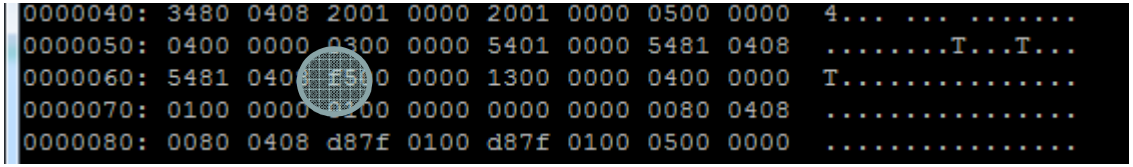
- Set byte offset 100 (i.e. Hex 0x64) of test.dat to 0xf5

$ xxd test.dat | less



$ echo –ne “\xf5” | dd of=test.dat count=1 bs=1 seek=100 conv=notrunc

$ xxd test.dat | less



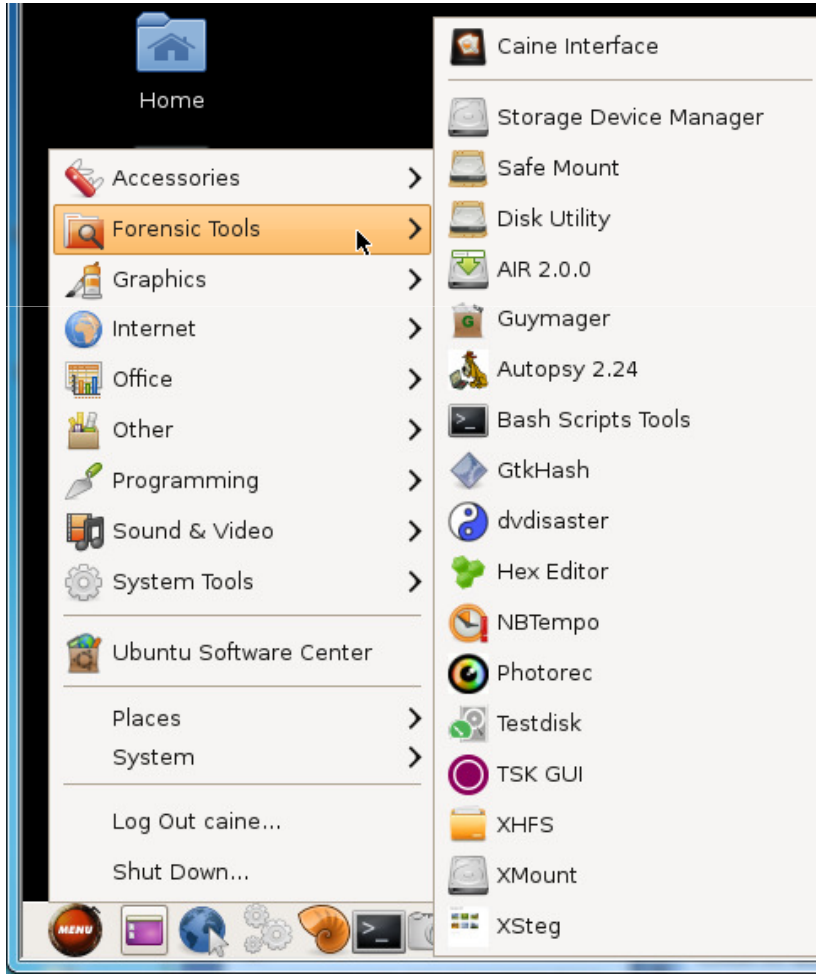
Edinburgh Napier UNIVERSITY

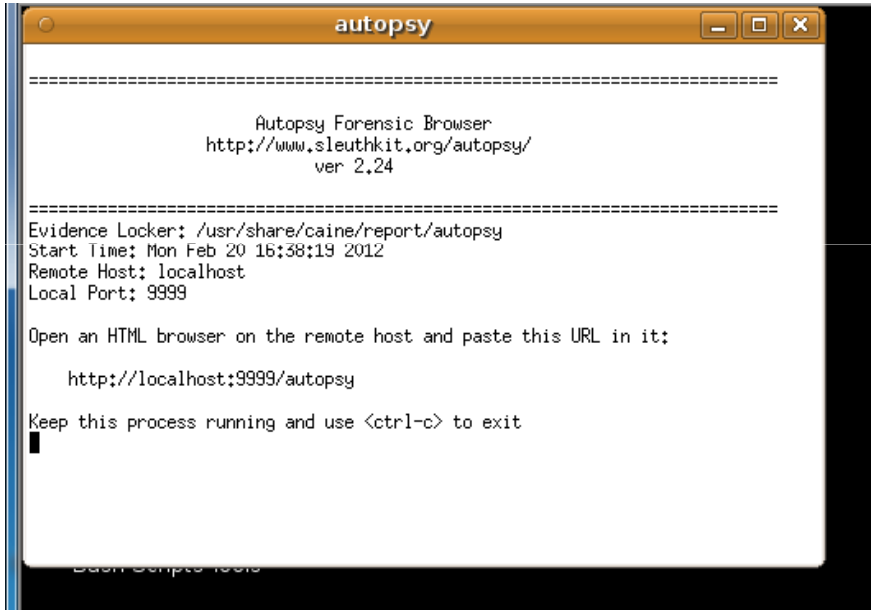
Autopsy

- Autopsy is a graphical interface to the Caine CLI tools.
- Autopsy does not have all the features of the Caine tools, or even all the tools.
- However, you may find it easier to use for some challenges.
- The practicals make you use both the CLI tools and Autopsy...

Edinburgh Napier UNIVERSITY

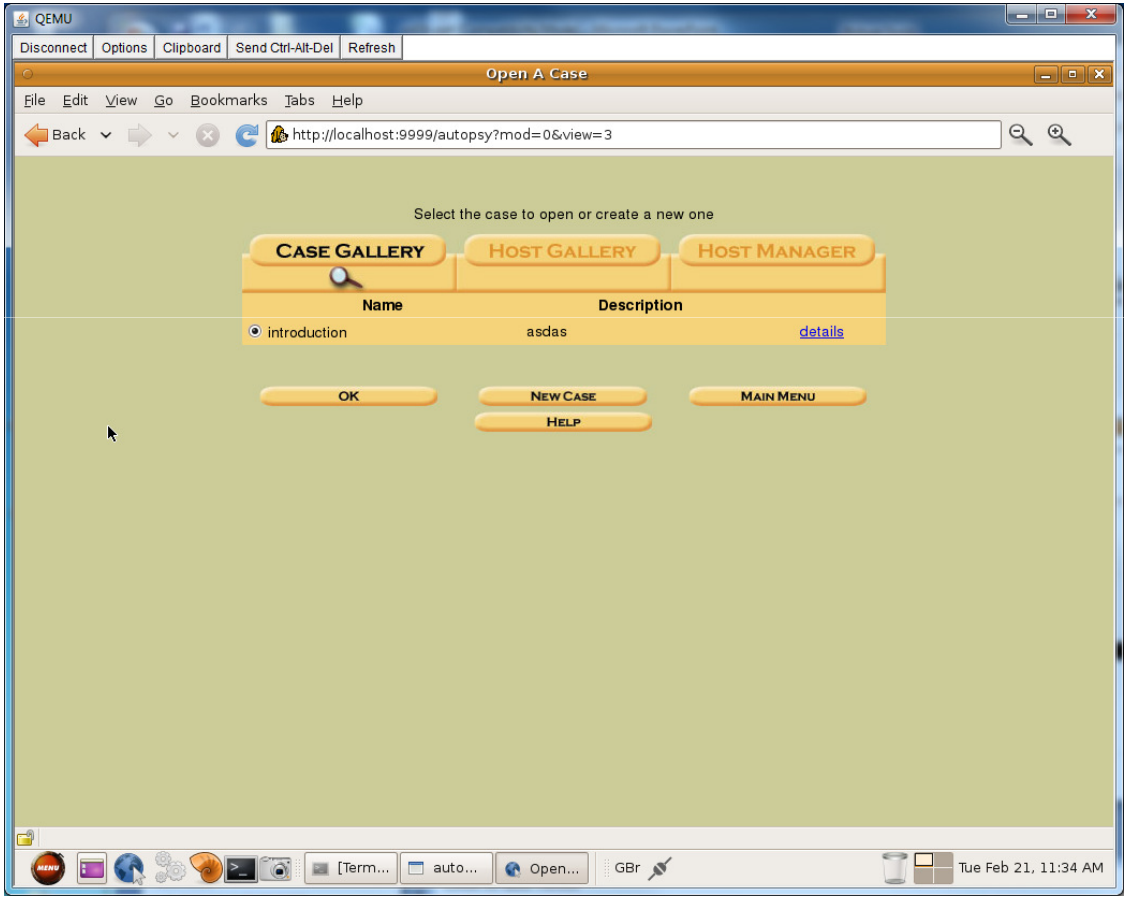
Run Autopsy 2.24





Browser Control

- Access via the browser within Caine itself...



Edinburgh Napier UNIVERSITY

Deleting Cases and Hosts

- You will need to create “cases” and “hosts”.
  - A case can have many different hosts in it
- If you make a mistake there is no delete key in Autopsy.
- But you can delete the cases and hosts from the normal command line...
- Cases are directories stored in
  - /usr/share/caine/report/autopsy
- A host in a case is a directory in the case directory. So for example a host HOST in case CASE is a directory:
  - /usr/share/caine/report/autopsy/CASE/HOST/
- To delete a directory and all its contents do:

  $ rm –rf /usr/share/caine/report/autopsy/WHATEVER

Edinburgh Napier UNIVERSITY

Next Week

- I have done my last lecture.
- From now on Robert will run the lectures.
- I will still be available in the practical sessions.

- Class test is week 8 in the practicals. Do not miss the test!

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

- Show a command line command which would set byte 561 of file hello.txt to 0x99.

Insert answer here:

Edinburgh Napier UNIVERSITY

Q2

- Consider the contents of the following file, “data.dat”

```
1;55;smith
2;10;jones
3;9;greg
4;199;allan
```

- Give a command line command which would sort this data by the second number in numerical order.

Insert answer here:

Edinburgh Napier UNIVERSITY

Q3

- Demonstrate a command line command to give a hex data dump of a file called “raw.dat”, but only showing bytes offsets10 to 20 inclusive.

Insert answer here: