

CSN08101

Digital Forensics

Lecture 5: Data management and Autopsy

Module Leader: Dr Gordon Russell

Lecturers: Robert Ludwiniak

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

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
```

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
```

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

- 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/lis | less

```

146.176.166.1 - PuTTY
0000000: 7f45 4c46 0101 0100 0000 0000 0000 0000  .ELF.....
0000010: 0200 0300 0100 0000 d09c 0408 3400 0000  .....4...
0000020: c893 0100 0000 0000 3400 2000 0900 2800  .....4. ... (
0000030: 1d00 1c00 0600 0000 3400 0000 3480 0408  .....4...4...
0000040: 3480 0408 2001 0000 2001 0000 0500 0000  4... ..
0000050: 0400 0000 0300 0000 5401 0000 5481 0408  .....T...T...
0000060: 5481 0408 1300 0000 1300 0000 0400 0000  T.....
0000070: 0100 0000 0100 0000 0000 0000 0080 0408  .....
0000080: 0080 0408 d87f 0100 d87f 0100 0500 0000  .....
0000090: 0010 0000 0100 0000 f08e 0100 f00e 0608  .....
00000a0: f00e 0608 dc03 0000 3010 0000 0600 0000  .....0.....
00000b0: 0010 0000 0200 0000 048f 0100 040f 0608  .....
00000c0: 040f 0608 e800 0000 e800 0000 0600 0000  .....
00000d0: 0400 0000 0400 0000 6801 0000 6881 0408  .....h...h...
00000e0: 6881 0408 4400 0000 4400 0000 0400 0000  h...D...D.....
00000f0: 0400 0000 50e5 7464 107f 0100 10ff 0508  ....P.td.....
0000100: 10ff 0508 2c00 0000 2c00 0000 0400 0000  ....,.....
0000110: 0400 0000 51e5 7464 0000 0000 0000 0000  ....Q.td.....
0000120: 0000 0000 0000 0000 0000 0000 0600 0000  .....
0000130: 0400 0000 52e5 7464 f08e 0100 f00e 0608  ....R.td.....
0000140: f00e 0608 1001 0000 1001 0000 0400 0000  .....
0000150: 0100 0000 2f6c 6962 2f6c 642d 6c69 6e75  ..../lib/ld-linu
0000160: 782e 736f 2e32 0000 0400 0000 1000 0000  x.so.2.....
:

```

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

```

146.176.166.1 - PuTTY
caine@host-19-17:~$ dd if=/images/usbimg1.dd skip=63 bs=512 count=1 | xxd
0000000: eb58 904d 5344 4f53 352e 3000 0201 c001  .X.MSDOSS.0....
0000010: 0200 0000 00f8 0000 3f00 ff00 3f00 0000  .....?..?..
0000020: c1af 0700 200f 0000 0000 0000 0200 0000  .....
0000030: 0100 0600 0000 0000 0000 0000 0000 0000  .....
0000040: 8000 29c4 ffd5 904e 4f20 4e41 4d45 2020  ..)...NO NAME
0000050: 2020 4641 5433 3220 2020 33c9 8ed1 bcf4  FAT32  3.....
0000060: 7b8e c18e d9bd 007c 884e 028a 5640 b441  {...|.N..V@.A
0000070: bbaa 55cd 1372 1081 fb55 aa75 0af6 c101  ..U.r...U.u...
0000080: 7405 fe46 02eb 2d8a 5640 b408 cd13 7305  t..F.-.V@...s.
0000090: b9ff ff8a f166 0fb6 c640 660f b6d1 80e2  ....f...@f....
00000a0: 3ff7 e286 cdc0 ed06 4166 0fb7 c966 f7e1  ?.....Af...f..
00000b0: 6689 46f8 837e 1600 7538 837e 2a00 7732  f.F...u8.~*.w2
00000c0: 668b 461c 6683 c00c bb00 80b9 0100 e82b  f.F.f.....+
00000d0: 00e9 2c03 a0fa 7db4 7d8b f0ac 84c0 7417  ....}).....t.
00000e0: 3cff 7409 b40e bb07 00cd 10eb eea0 fb7d  <.t.....)
00000f0: ebe5 a0f9 7deb e098 cd16 cd19 6660 807e  ....}.....f`~
0000100: 0200 0f84 2000 666a 0066 5006 5366 6810  .... .fj.fP.Sfh.
0000110: 0001 00b4 428a 5640 8bf4 cd13 6658 6658  ....B.V@....fXfX
0000120: 6658 6658 eb33 663b 46f8 7203 f9eb 2a66  fXfX.3f;F.r...*f
0000130: 33d2 660f b74e 1866 f7f1 fec2 8aca 668b  3.f..N.f.....f.
0000140: d066 c1ea 10f7 761a 86d6 8a56 408a e8c0  .f...v...V@...
0000150: e406 0acc b801 02cd 1366 610f 8275 ff81  .......fa..u..
0000160: c300 0266 4049 7594 c342 4f4f 544d 4752  ...f@Iu..BOOTMGR
0000170: 2020 2020 0000 0000 0000 0000 0000 0000  .....
0000180: 0000 0000 0000 0000 0000 0000 0000 0000  .....
0000190: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00001a0: 0000 0000 0000 0000 0000 0000 0d0a 5265  .....Re
00001b0: 6d6f 7665 2064 6973 6b73 206f 7220 6f74  move disks or ot
00001c0: 6865 7220 6d65 6469 612e ff0d 0a44 6973  her media...Dis
00001d0: 6b20 6572 726f 72ff 0d0a 5072 6573 7320  k error...Press
00001e0: 616e 7920 6b65 7920 746f 2072 6573 7461  any key to resta
00001f0: 7274 0d0a 0000 0000 00ac cbd8 0000 55aa  rt.....U.
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.00135755 s, 377 kB/s
caine@host-19-17:~$

```

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

```
0000030: 1d00 1c00 0600 0000 3400 0000 3480 0408  .....4...4...
0000040: 3480 0408 2001 0000 2001 0000 0500 0000  4... ..
0000050: 0400 0000 0300 0000 5401 0000 5481 0408  .....T...T...
0000060: 5481 0408 0200 0000 1300 0000 0400 0000  T.....
0000070: 0100 0000 0200 0000 0000 0000 0080 0408  .....
```

\$ echo -ne "\xf5" | dd of=test.dat count=1 bs=1 seek=100 conv=notrunc

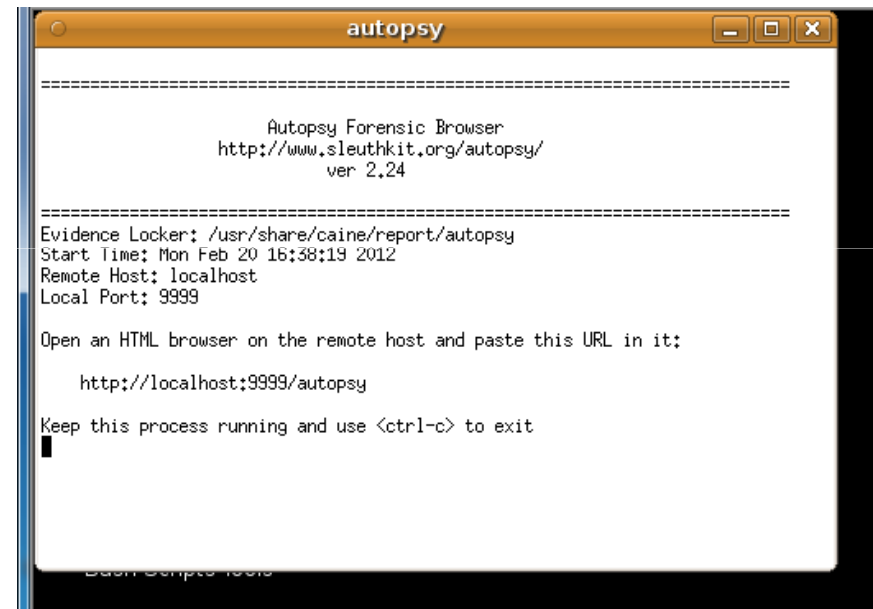
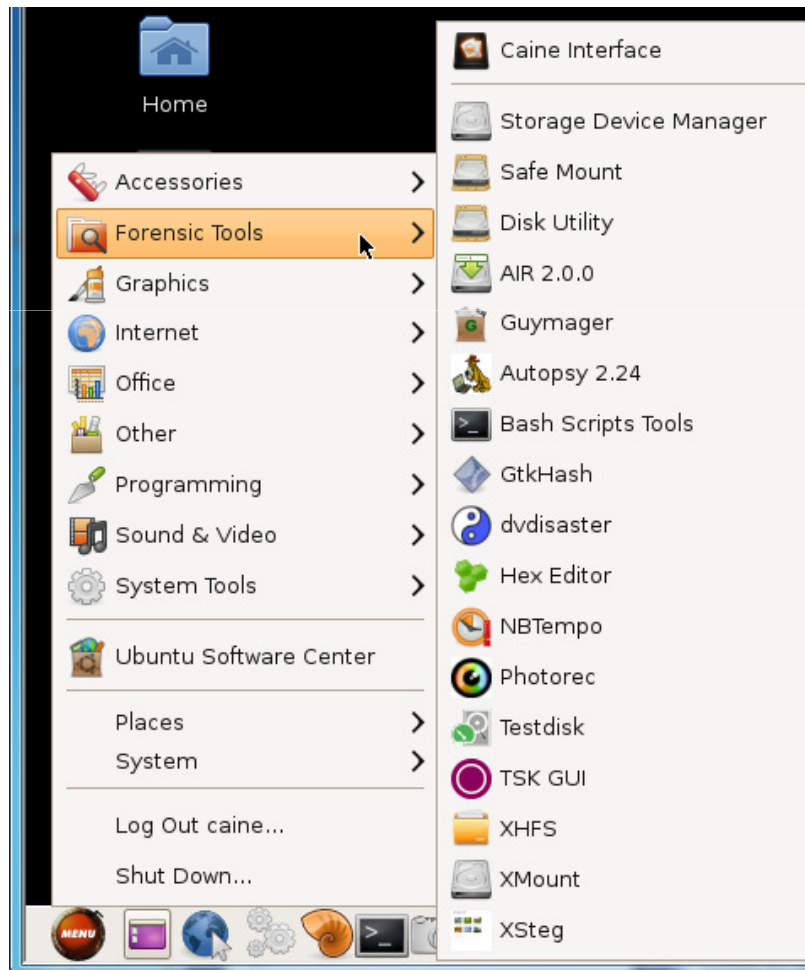
\$ xxd test.dat | less

```
0000040: 3480 0408 2001 0000 2001 0000 0500 0000  4... ..
0000050: 0400 0000 0300 0000 5401 0000 5481 0408  .....T...T...
0000060: 5481 0408 0200 0000 1300 0000 0400 0000  T.....
0000070: 0100 0000 0200 0000 0000 0000 0080 0408  .....
```

Autopsy

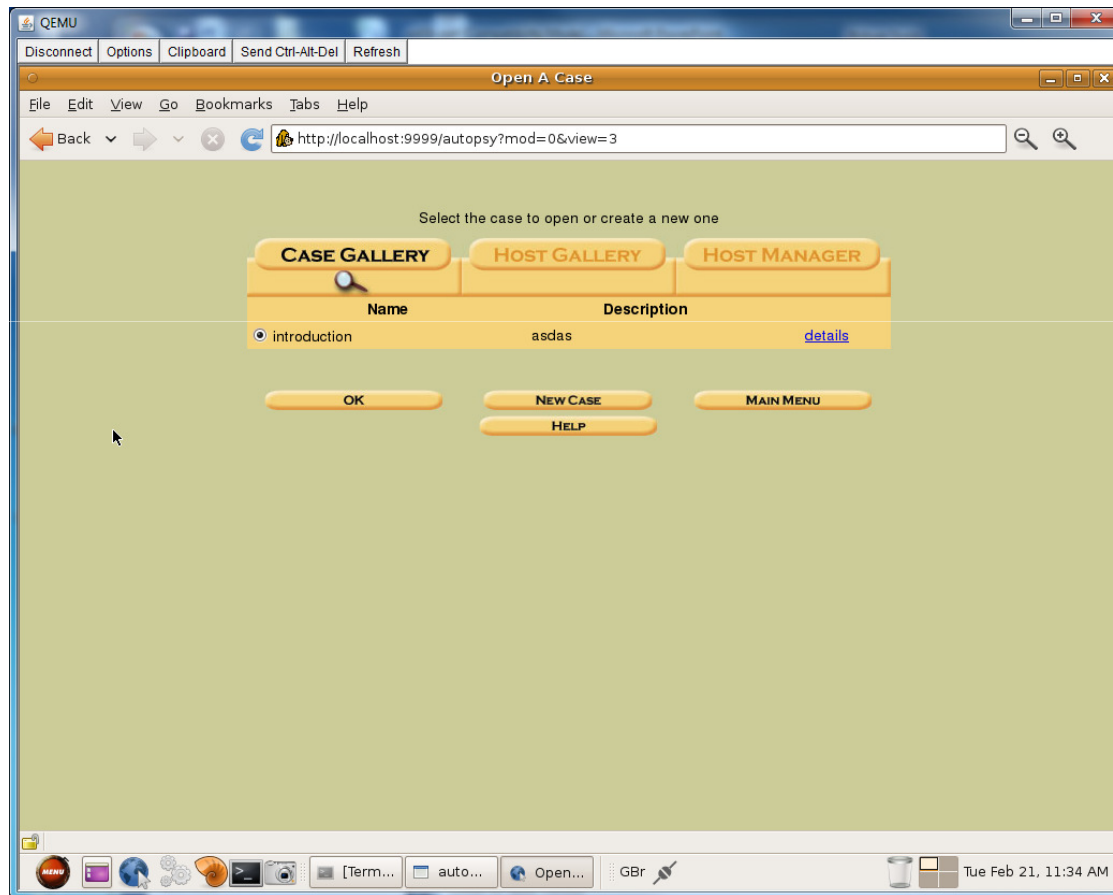
- Autopsy is a graphical interface to the Caine CLI tools.
- Autopsy does not have all the features of the Caine tools, or even all the tools.
- However, you may find it easier to use for some challenges.
- The practicals make you use both the CLI tools and Autopsy...

Run Autopsy 2.24



Browser Control

- Access via the browser within Caine itself...



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`

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!



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.

Q1

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

Insert answer here:

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:

Q3

- Demonstrate a command line command to give a hex data dump of a file called “raw.dat”, but only showing bytes offsets 10 to 20 inclusive.

Insert answer here: