Cardiff University

CM3105 Security and Forensics

Computer Forensics Assignment 2013 - Technical Report

Student Name:
Geraint Harries
Student Number:
1100682

Lecturer(s):
Mike Daley

December 10, 2013

1 Abstract

1.1 Tasking

For this assignment, we were tasked to analyse a USB image for evidence indicating the individual has been involved in industrial espionage against DataLog INc..

1.2 Executive Summary

This report will show evidence to suggest that Mona Simpson was involved with industrial espionage. Her role within DataLog Inc. allowed her to access information and supply it to *'Ned'* (surname unknown).

2 Preperation

2.1 File Integrity

I was given an image of the USB entitled fishytails.dd. The first thing I did was make a MD5 and an SHA hash of the image.

MD5 Hash Value: 2cea312fd83da54140717a4830fb33bf
SHA Hash Value: 54289cb3bfb8666d4d1836dd05ab74a13f1c8e19

I make a copy of the image and named it fishytails.dd. I ran the hash functions on this to verify the copy had been totally successful. I then made the copy read only by running the command.

chmod 400 fishtailscopy.dd

I then verified it by listing the directory permissions using the ls - l command. This gave the following output:

-r——— 1 forensic forensic 473563136 Nov 22 20:09 fishytailscopy.dd

This allows me to investigate the data without touching the original image, thus eliminating the possibility of contamination.

2.2 Autopsy

I created a new case in autopsy, entitled DataLogIncInvestigation. I then added a new host, entitled MonaSimpsonUSB. I added the fishytailscopy.dd to the case as a partition. I then verified the hash to check data integrity.

3 Investigation

3.1 Creating a Timeline

Using autopsy, I created a timeline. I did not enter a starting or end date (See Appendix 8.3, Figures 1,2,3 and 4 for full timeline table). You can see from the table that the creation date for all the files and directories is 1970, whereas the modification and access date is 2012. This suggests that the system clock of the original directory and filelocation have been tampered with.[1]

From the timeline, we can see several file and directory names. This will help us build a dirty word list (See Appendix 8.1)

3.2 Media Analysis

Using the File Analysis tool within Aytopsy, I was able to step through the directories of the image and see all the files both present and deleted. Appendix 8.3, Figure 5, shows the directory structure of the USB image.

In the directory *My Tank/Documents*, I found a file called *Shopping List.xls*. Although the *.xls* suffix implies it is encoded with the Microsoft Excel File format, the metadata shown by autopsy shows that the file was originally created using Microsoft Office Word (See Appendix 8.3, Figure 6). I changed the suffix of the document to *.doc*, Appendix 8.3, Figure 7 shows the documents as it was created. The message says

> Hi,
> I got it, its with angle fish, you know what to do, just run it through snake.
> Ned

[1] This could also be an unwanted remnant of creating the USB image for this coursework.

Ned is now someone we can identify as implicated. We can add the name *Ned* to our dirty word list, as well as snake.[2]. A deleted file within the same directory *_i.xls*, also contains the message.

Within *My Tanks/Documents/progs/for your eyes only/* there is a deleted python script called _nake.py (See Appendix 8.3, Figure 8 and 9). Given the content of *Shopping List.xml* when encoded with *.doc* format, it's fair to assume that the deleted character is *s*. This script takes the file *combined.ppm*, decrypts it and returns the file *decrypted.ppm*. This suggests that that an image *combined.ppm* exists and that it contains secret content.

In *My Tank/Marines/My new Aquarium/new fish/* there are 4 images, three of which is deleted. The files are called, *_ombined.png, _ombined.ppm, AngleFish.png, AngleFish.ppm*. It is fair to assume the missing characters of the first two files are c. *combined.ppm* is the desired input for the script *_nake.py*. We can therefor assume that the script was intended to be used.

I ran both *.ppm* files through the *_nake.py* file. *_ombined.ppm* was unable to be decrypted however, *AngleFish.ppm* was able to be and generated an image (See Appendix 8.3, Figure 11). The image *AngleFish.ppm* uses steganography which means that one file can be contained within another. This is what has been done here. The generated image in Appendix 8.3, Figure 11, is what was hidden within *AngleFish.ppm*.
There are many other images of fish on the drive however I found no evidence to suggest that any steganographic techniques were used. I investigated these files however found no evidence to suggest they were worth reporting.

4 String Search

For the string search, I searched all the terms in the dirty words list (See Appendix 8.1). I searched the terms in the dirty word list without case sensitivity and showing the terms in ascii and unicode. I did not do a grep regular expression search. The results for the string search of the terms

[2]This answers part 1 of the basic requirements of the coursework. There is someone else implicated he is known as *ned*

Angle, Fish, Ned and *Snake* are shown in Appendix 8.3 figures 19, 20, 21 and 22 respectively. The results did not show us anything that we hadn't seen before.

5 Evidence

5.1 Shopping List.xls

Evidence Number	001
File Name	Shopping List.xls
File Path	C:/My Tank/Documents/
Date/ Time Created	Sun April 14 21:53:58 2013
Created Using	Microsoft Office Word
Additional Information	n/a
Summary	A file encoded using Microsoft Office Word but displayed with Microsoft Office Excel
MD5 Hash	03c633e3ae39bfd27a59c2e2041eebd4
Figure Reference	Appendix 8.3, Figure 7 and 12

5.2 _nake.py

Evidence Number	002
File Name	_nake.py
File Path	C:/My Tank/Documents/progs/
Date/ Time Created	Sun April 14 21:53:58 2013
Created Using	Unkown
Additional Information	It had been deleted
Summary	A python script which decrpts an image using steganographic techniques
MD5 Hash	6fc0ed465f263bf06a10894b7a9a13
Figure Reference	Appendix 8.3, Figure 8 and 9

5.3 AngleFish.ppm

Evidence Number	003
File Name	AngleFish.ppm
File Path	C:/My Tank/Marines/My new Aquarium/
Date/ Time Created	Sun April 17 11:49:47 2013
Created Using	Unkown
Additional Information	n/a
Summary	Image of two fish
MD5 Hash	75f051e14ef0ed7c19cf4c04ab13d174
Figure Reference	Appendix 8.3, Figure 13

5.4 decrypt.ppm

Evidence Number	004
File Name	decrypt.ppm
File Path	
Date/ Time Created	
Created Using	_nape.py
Additional Information	This image was generated on my machine. It was embedded within the image AngleFish.ppm using steganography.
Summary	An image containing a phone attached to a circuit board
MD5 Hash	01bd7e725008c55f60e999e9add4149d
Figure Reference	Appendix 8.3, Figure 11

5.5 combined.ppm

Evidence Number	005
File Name	combined.ppm
File Path	C:/Nothing Here to see/New folder/New folder/new fish/New folder/
Date/ Time Created	Sun April 14 21:53:59 2013
Created Using	Unknown
Additional Information	This image uses steganography to hide the image decrypt.ppm
Summary	Image of two fish
MD5 Hash	75f051e14ef0ed7c19cf4c04ab13d174
Figure Reference	Appendix 8.3, Figure 14

5.6 _i.xls

Evidence Number	006
File Name	_i.xls
File Path	C:/My Tank/Documents/
Date/ Time Created	Sun Apr 14 21:53:58
Created Using	Unknown
Additional Information	It has been deleted
Summary	File containing text
MD5 Hash	d231d480ebc0b06ef3c51094ca7c99d0
Figure Reference	Appendix 8.3, Figure 15

5.7 Questions specifically asked

5.7.1 Is there anyone else implicated?

In section 3.2, I highlight that *Ned* (Surname unknown) is implicated.

5.7.2 Where is Penelope planning to travel to?

In the IP packets supplied by DataLog Inc. Mona is messaging someone. The message says:

> Here's the secret recipe. I just downloaded it from the file server. Just copy to a thumb drive and you're good to go :-).

The person then replies

See you in hawaii!

This implies that Mona will be travelling to Hawaii soon.

5.7.3 Can you find the stolen photo?

Section 3.2 explains how I found the stolen photo

5.7.4 How was the file hidden and how did you recover it?

Section 3.2 explains how the image was hidden.

5.7.5 What other steps have been taken (if any) have been taken to hide evidence?

They have deleted several files, this is shown in section 6. They have also tried to hide files in the depths of sub folders.

6 Deleted Files

I used the *All Deleted Files* function within Autopsy to find all the deleted files from the image.

6.1 _i.xls

Evidence Number	006
File Name	_i.xls
File Path	C:/My Tank/Documents/
Date/ Time Created	Sun Apr 14 21:53:58
Created Using	Unknown
Additional Information	It has been deleted
Summary	File containing text
MD5 Hash	d231d480ebc0b06ef3c51094ca7c99d0
Figure Reference	Appendix 8.3, Figure 15

6.2 _nake.py

Evidence Number	002
File Name	_nake.py
File Path	C:/My Tank/Documents/progs/
Date/ Time Created	Sun Apr 14 21:53:58 2013
Created Using	Unkown
Additional Information	It had been deleted
Summary	A python script which decrpts an image using steganographic techniques
MD5 Hash	6fc0ed465f263bf06a10894b7a9a13
Figure Reference	Appendix 8.3, Figure 8 and 9

6.3 _ombined.png

Evidence Number	007
File Name	_ombined
File Path	C:/My Tank/Marines/My new Aquarium/new fish/Something fishy/
Date/ Time Created	Sun Apr 14 21:53:59 2013
Created Using	Unkown
Additional Information	It had been deleted
Summary	Image of two fish
MD5 Hash	0a1cb58285957988d523cc6eff08254f
Figure Reference	Appendix 8.3, Figure 16

6.4 AngleFish.png

Evidence Number	008
File Name	AngleFish.png
File Path	C:/My Tank/Marines/My new Aquarium/new fish/Something fishy
Date/ Time Created	Sun April 14 21:53:59 2013
Created Using	Unkown
Additional Information	n/a
Summary	Image of two fish
MD5 Hash	0a1cb58285957988d523cc6eff08254f
Figure Reference	Appendix 8.3, Figure 17

6.5 _ombined.ppm

Evidence Number	009
File Name	_ombined.ppm
File Path	C:/My Tank/Marines/My new Aquarium/new fish/Something Fishy/
Date/ Time Created	Sun Apr 17 11:49:47 2013
Created Using	Unkown
Additional Information	n/a
Summary	A series of numbers
MD5 Hash	b6e0f5979181a3f46dfddacbf4de5b56
Figure Reference	Appendix 8.3, Figure 18

7 Summary

I made a MD5 hash of the image after I had finished investigating.
MD5 Hash: 2cea312fd83da54140717a4830fb33bf
This matches the first MD5 hash, meaning that the integrity of the image remains.
The evidence suggests that she was involved with industrial espionage as some images on the USB image use stegonography to hide evidence and many files have been deleted to hide information from law enforcement agencies.

8 Appendix

8.1 Dirty Word List

- Angle
- Fish
- Snake
- Ned

8.2 Tools Used

- Autopsy

- Vim
- Libre Office

Autopsy automated a lot of unix commands, it seemed the obvious choice for a quick analysis. Vim is a terminal text editor which I used to view some of the files in. Libre Office was useful to view *Shopping List* in and viewing it with different suffixes.

8.3 Figures

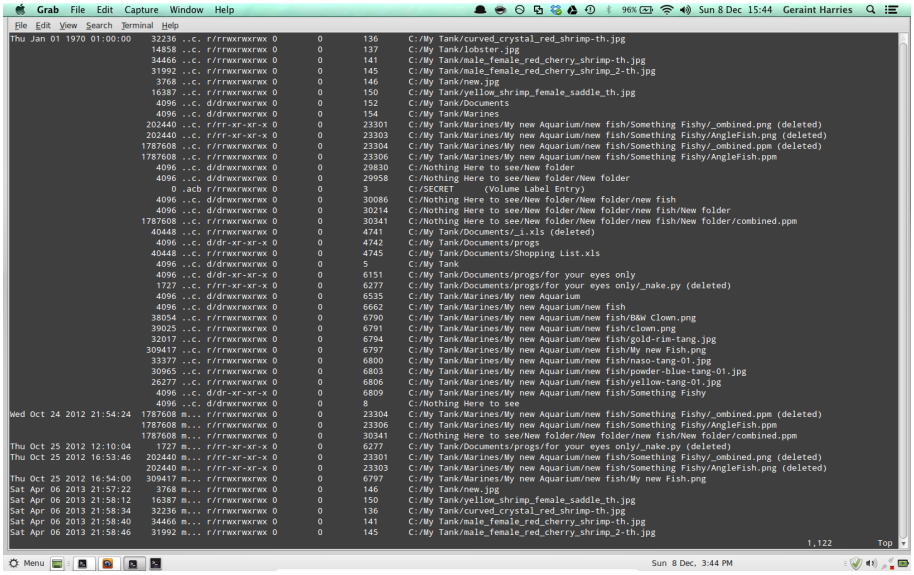

Figure 1: Timeline Page 1

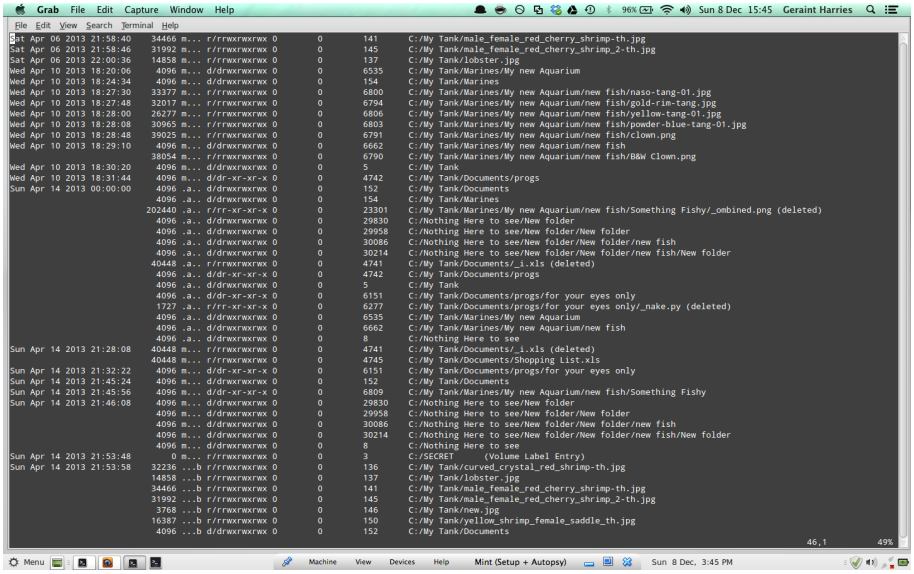

Figure 2: Timeline Page 2

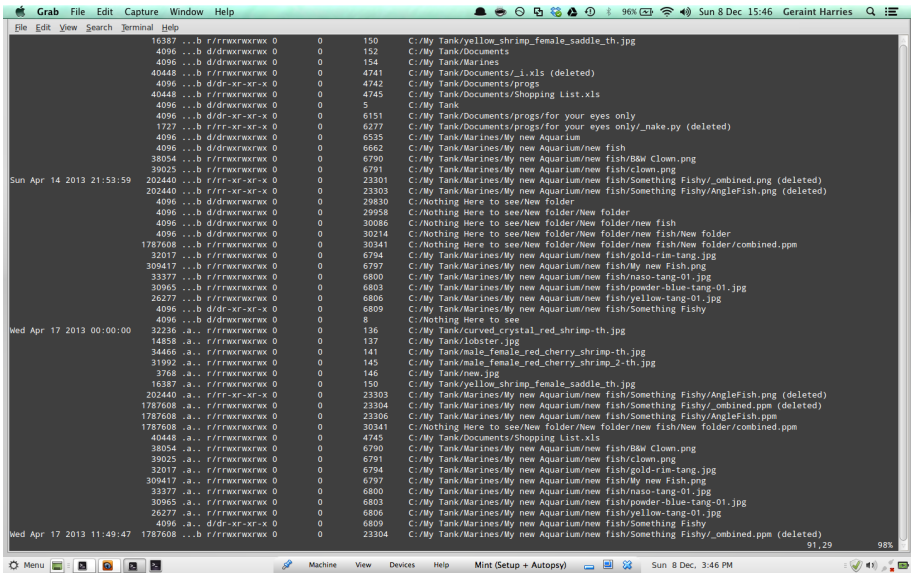

Figure 3: Timeline Page 3

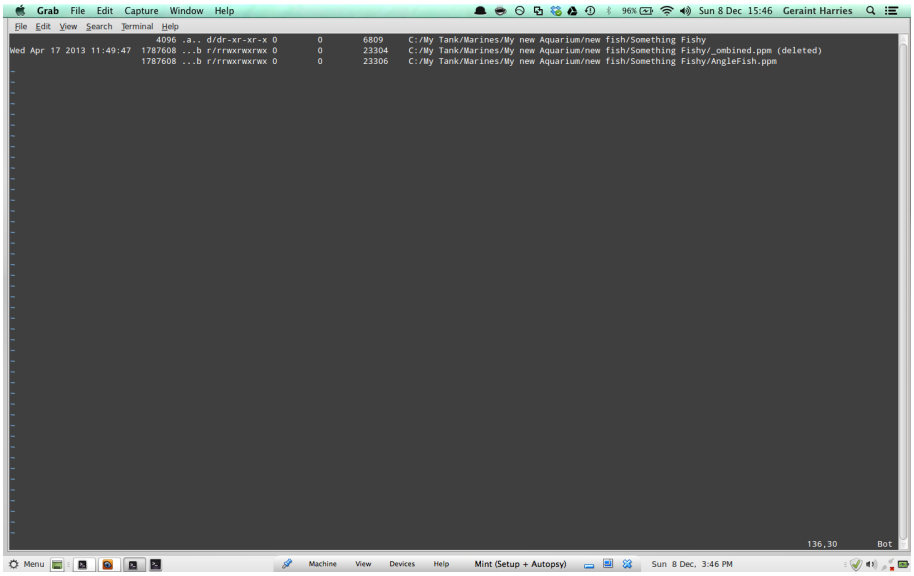

Figure 4: Timeline Page 4

$FAT1
:
$FAT2
:
$MBR
:
$Orphan Files
:
My Tank
:
.....Documents
: :
: .....progs
: :
: .....for your eyes only
:
.....Marines
: :
: .....My New Aquarium
: :
: ..... New Fish
: :
: .....Something Fishy
:
Nothing Here To See
:
.....New Folder
: :
: .....New Folder
: :
: .....New Fish
: :
: .....New Folder
:
SECRET

Figure 5: Directory Structure

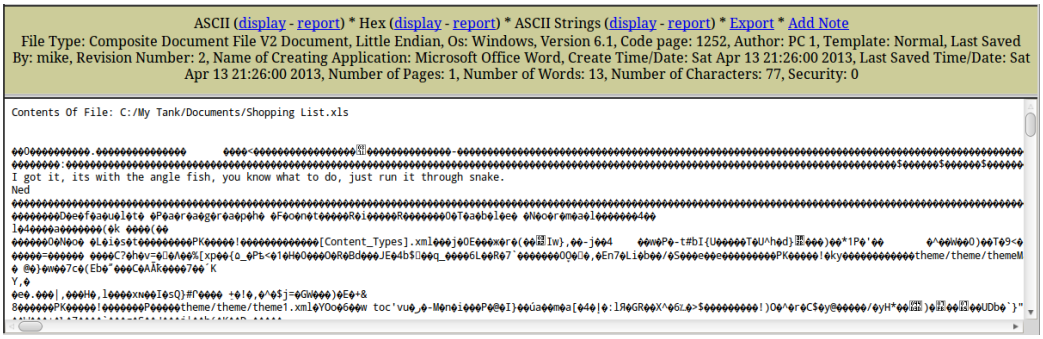

Figure 6: Shopping List.xls contents and metadata

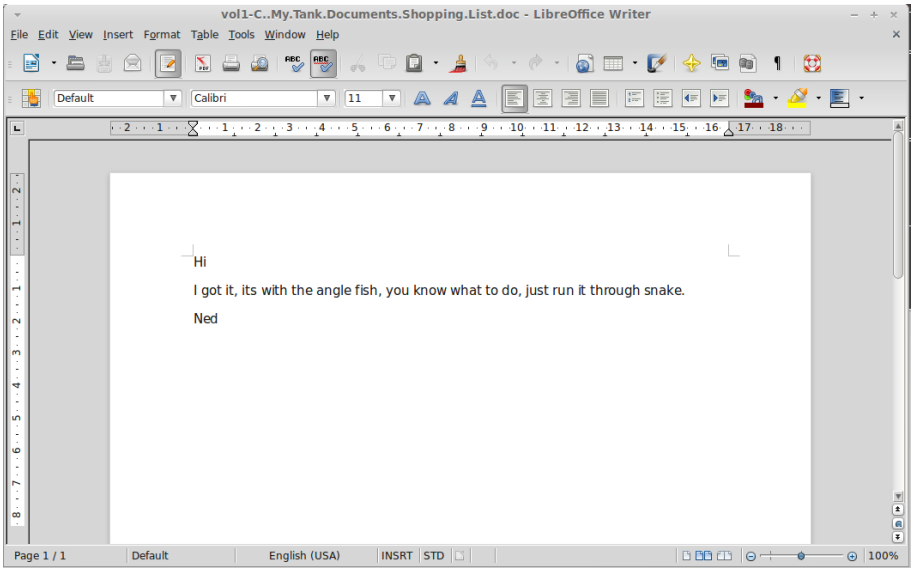

Figure 7: Shopping List.xls encoded as a .doc file

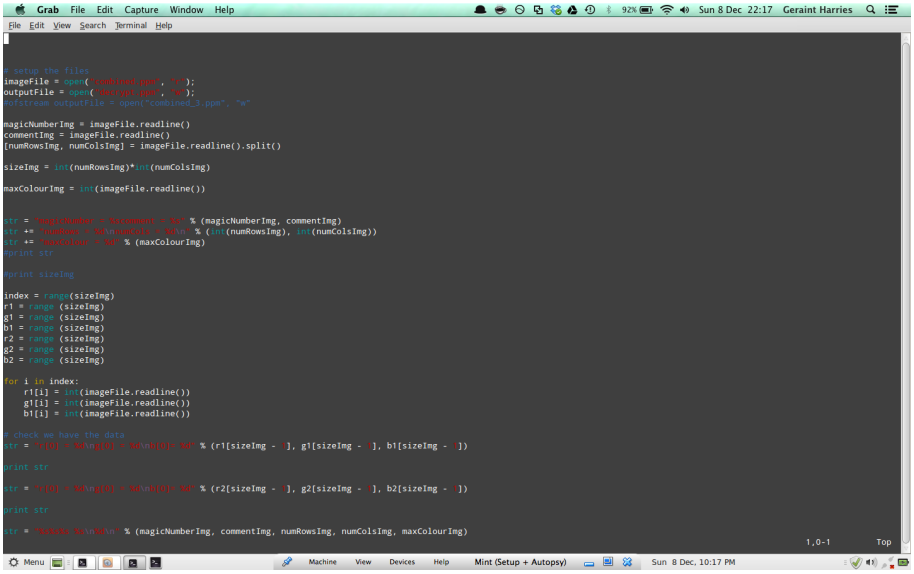

Figure 8: _nape.py Page 1

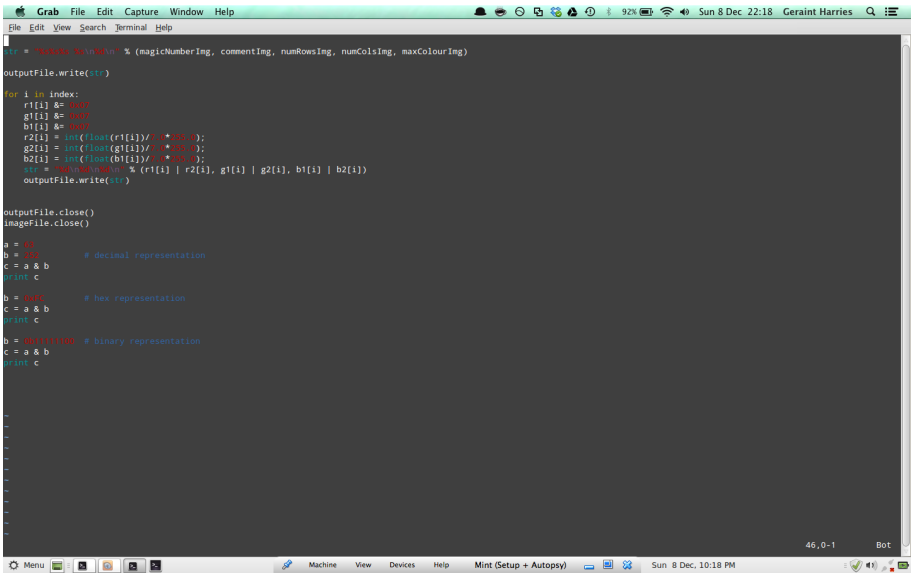

Figure 9: _nape.py Page 2

Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
	d / d	../	2013-04-10 18:29:10 (BST)	2013-04-14 00:00:00 (BST)	2013-04-14 21:53:58 (BST)	4096	0	0	6662
	d / d	./	2013-04-14 21:45:56 (BST)	2013-04-17 00:00:00 (BST)	2013-04-14 21:53:59 (BST)	4096	0	0	6809
✔	r / r	_ombined.png	2012-10-25 16:53:46 (BST)	2013-04-14 00:00:00 (BST)	2013-04-14 21:53:59 (BST)	202440	0	0	23301
✔	r / r	_ombined.ppm	2012-10-24 21:54:24 (BST)	2013-04-17 00:00:00 (BST)	2013-04-17 11:49:47 (BST)	1787608	0	0	23304
✔	r / r	AngleFish.png	2012-10-25 16:53:46 (BST)	2013-04-17 00:00:00 (BST)	2013-04-14 21:53:59 (BST)	202440	0	0	23303
	r / r	AngleFish.ppm	2012-10-24 21:54:24 (BST)	2013-04-17 00:00:00 (BST)	2013-04-17 11:49:47 (BST)	1787608	0	0	23306

Figure 10: 4 files, 3 of which are deleted

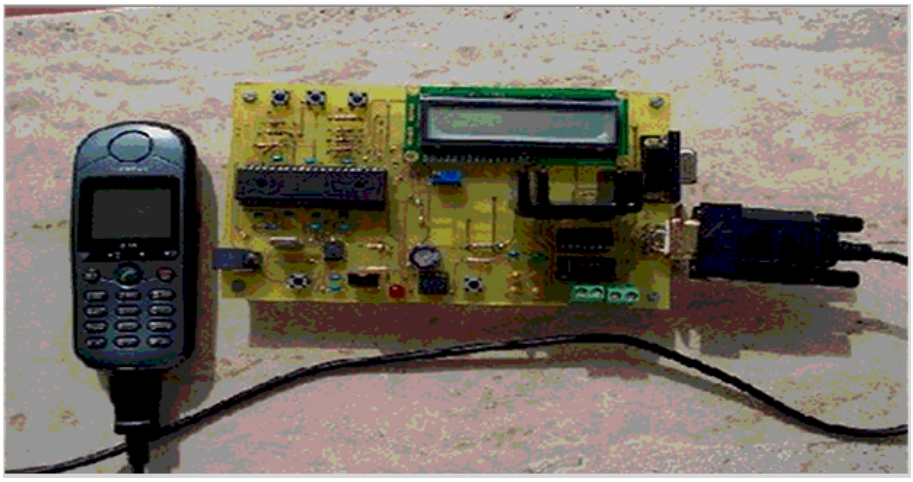

Figure 11: This image was generated by running AngleFish.ppm through the _nape.py script

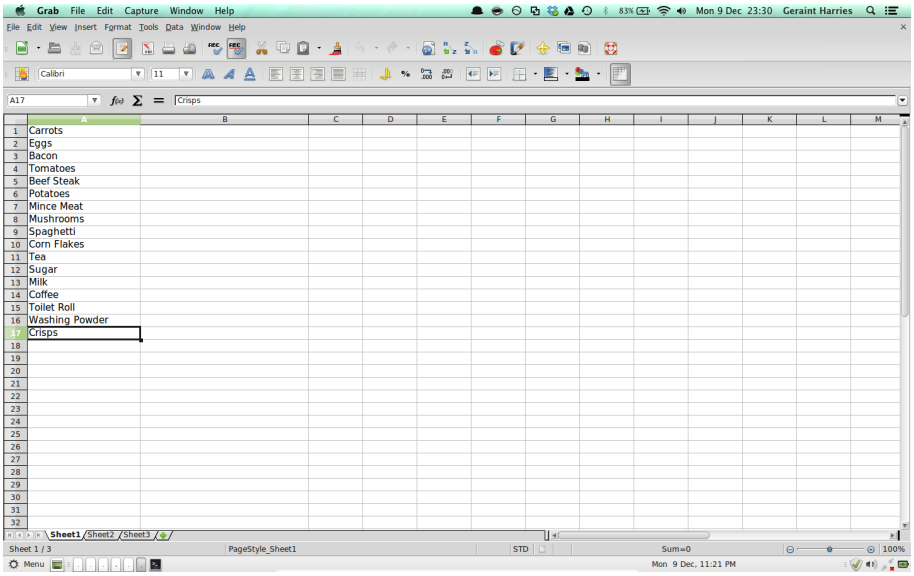

Figure 12: Shopping List.xls encoded as a .xls file

Figure 13: AngleFish.ppm

Figure 14: Combined.ppm

Contents Of File: C:/My Tank/Documents/_i.xls

I got it, its with the angle fish, you know what to do, just run it through snake.
Ned

Figure 15: _i.xls

Figure 16: _ombined.png

Figure 17: AngleFish.png

Figure 18: _ombined.ppm

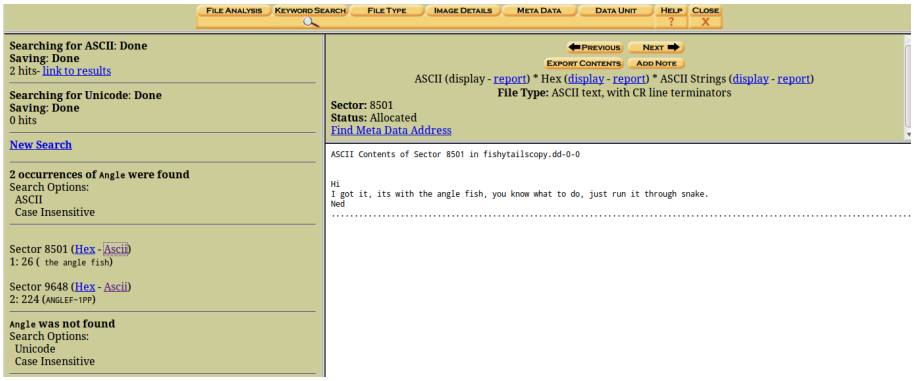

Figure 19: The keyword search results for searching the term *Angle*

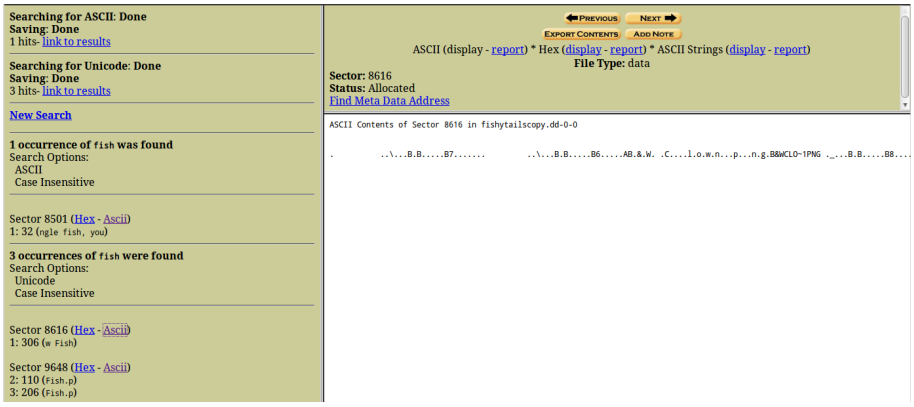

Figure 20: The keyword search results for searching the term *Fish*

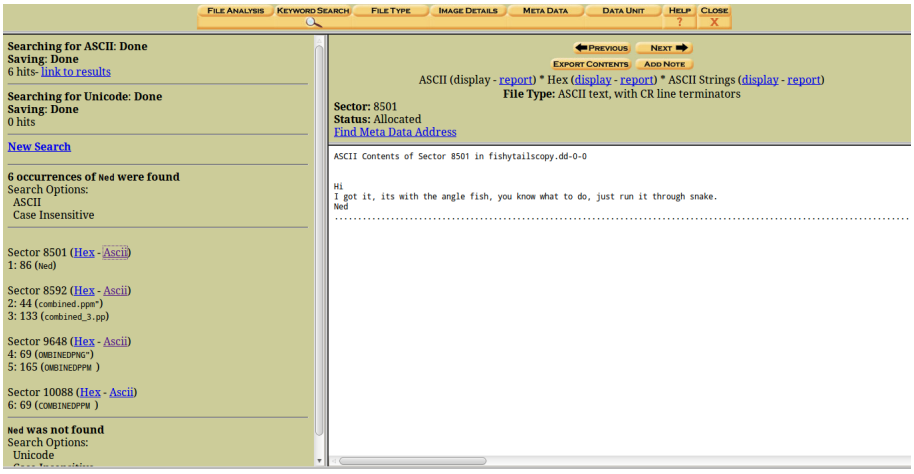

Figure 21: The keyword search results for searching the term *Ned*

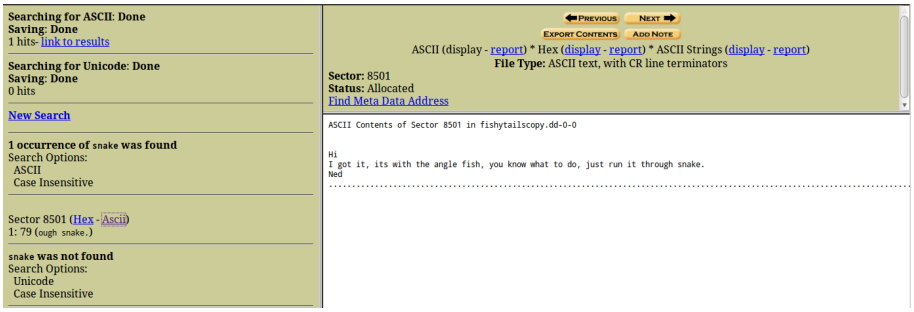

Figure 22: The keyword search results for searching the term *Snake*