Cardiff University

CM3105 Security and Forensics

Computer Forensics Assignment 2013 - Lamens Report

Student Name:
Geraint Harries
Student Number:
1100682

Lecture(s):
Mike Daley

December 11, 2013

1 Abstract

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.

2 Analysis

Appendix 1, Figure 1 contains an image of the folders contained on the USB. (FAT1, FAT2, MBR and OrphanFiles there are required files on every USB). Within *Documents*, there is a file entitled *Shopping List.xls* (See Section 3.1.1). This file has a hidden file within it. If you change the name of the file from *Shopping List.xls* to *Shopping List.doc*, it will show a different message. (See Appendix 1, Figures 2 and 3)

The file contains the message

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

Ned is now someone we can identify as implicated. Another file within *Documents* contains this message (See section 3.1.6 and Appendix 1, figure 4). Within *My Tanks/Documents/progs/for your eyes only/* there is a deleted file called *_nake.py* (See Appendix 1, Figures 5 and 6 and Section 3.1.2). Given the content og *Shopping List.xls* when it has *.doc* at the end, we can assume the deleted character is *S*. The script takes the file *combined.ppm*, decrypts it and returns te file *decrypted.ppm*. This suggests that the file *combined.ppm* exists and contains secret information
In *My Tank/Marines/My new Aquarium/new fish/* there are 4 images, three of which are deleted. The files called, *_omined.png, _ombined.ppm, AngleFish.png, AngleFish.ppm* (See Appendix 1, Figures 7, 8, 9 and 10 and Section 3.1.7, 3.1.9, 3.1.8 and 3.1.3). It's fair to assume the missing characters of the first two files are c. *combined.ppm* is the desired input for the script *_nake.py*. From these images, we can assume it 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 1, Figure 11 and Section 3.1.3). This image *AngleFish.ppm* uses a coding system to hide another image within it.

There are many other images of fish on the drive, however I found no evidence to suggest that any coding techniques were used. I investigated these files and found no evidence.

The evidence supplied by DataLog Inc. suggests that Mona Simpson may be travelling to Hawaii soon. She sent a message saying

> 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 is implies that Mona will be travelling to Hawaii soon.

3 Evidence

Appropriate measures were taken to ensure the evidence was not compromised by my investigation. For more details please see the attacked technical report.

3.1 Evidence

3.1.1 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 1, Figure 2 and 3

3.1.2 _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 1, Figure 5 and 6

3.1.3 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 1, Figure 9

3.1.4 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 1, Figure 11

3.1.5 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	NO REF

3.1.6 _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 1, Figure 4

3.1.7 _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 1, Figure 7

3.1.8 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 1, Figure 10

3.1.9 _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 1, Figure 8

4 Overall Opinion

Therefore, I believe that there is evidence to suggest that Mona Simpson has been taking part in industrial espionage. Her position within the company gave her the opportunity to access the information. Given the extent she has gone to, to hide this, it suggests she didn't want government agencies or DataLog Inc. to see what she was doing. The evidence also shows another individual *Ned* (Surname unknown) is part of this operation.

5 Appendix

5.1 Figures

$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 1: Directory Structure

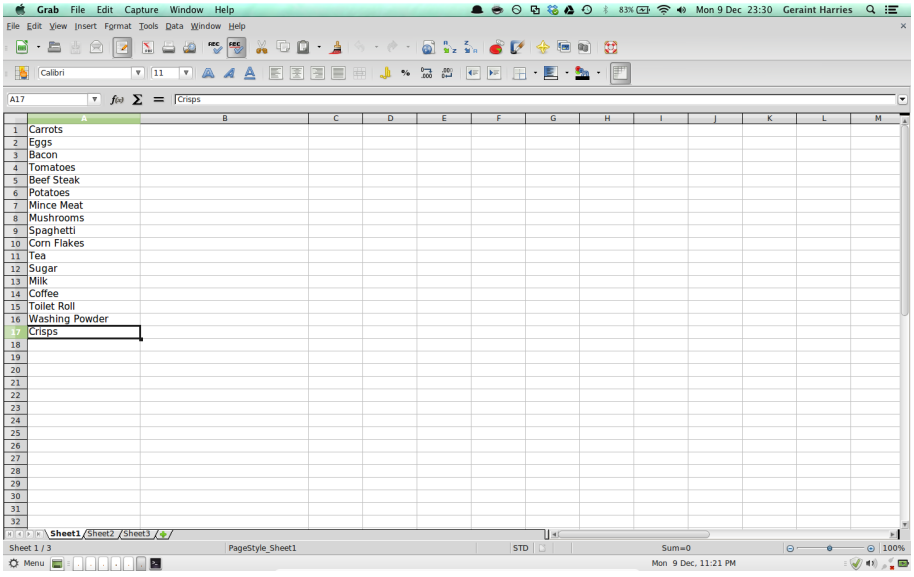

Figure 2: Shopping List.xls with .xls at the end

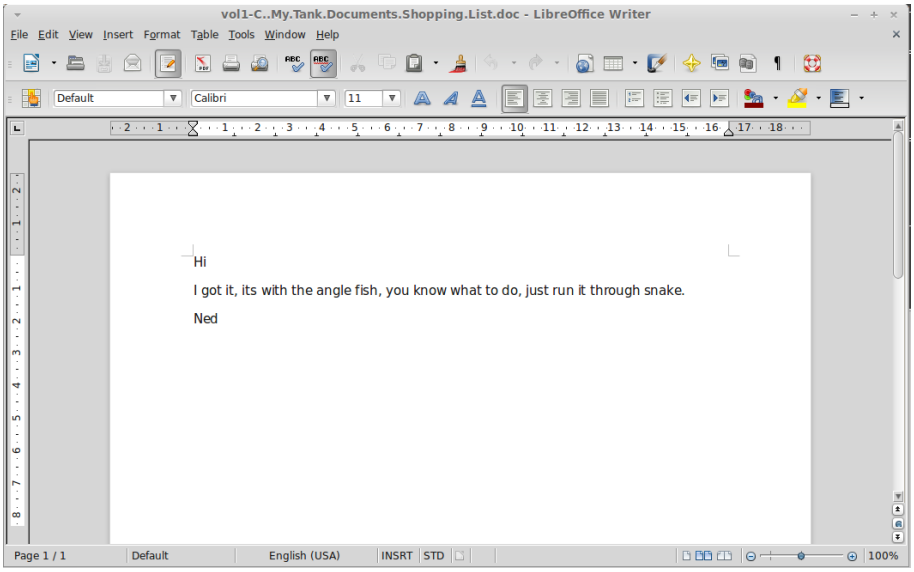

Figure 3: Shopping List.xls with .doc at the end i.e. Shopping List.doc

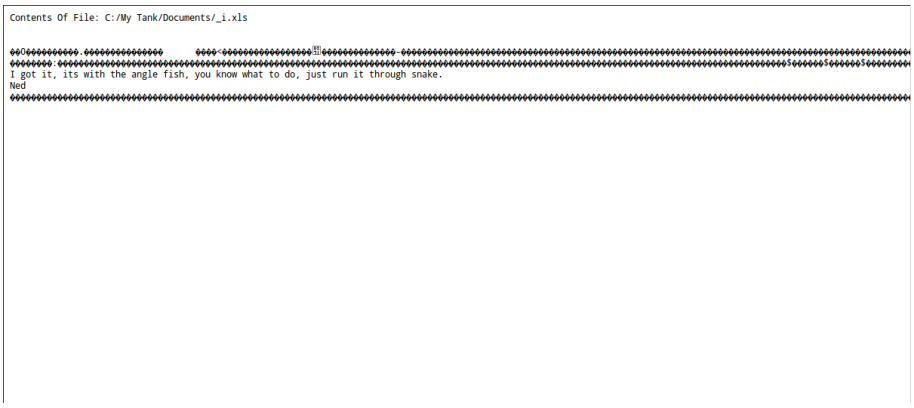

Figure 4: _i.xls

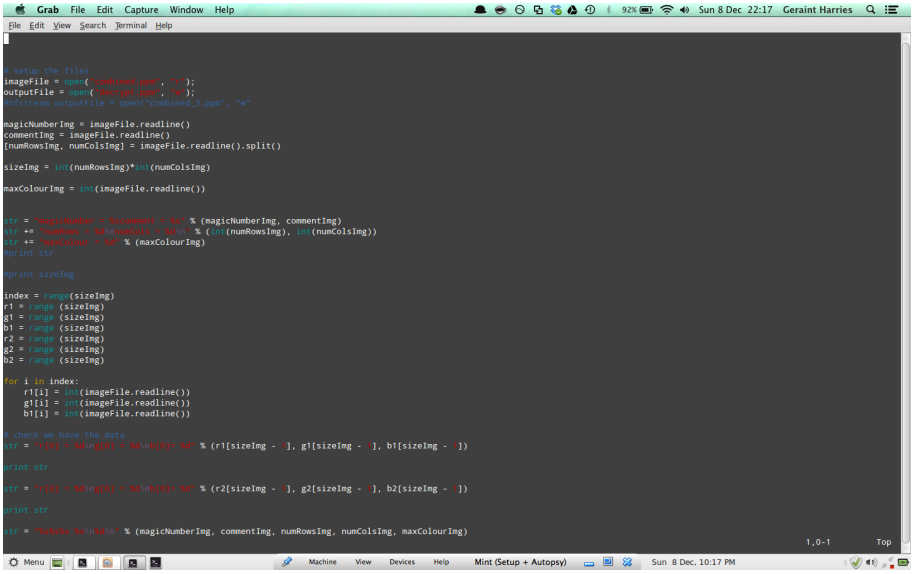

Figure 5: _nake Page 1

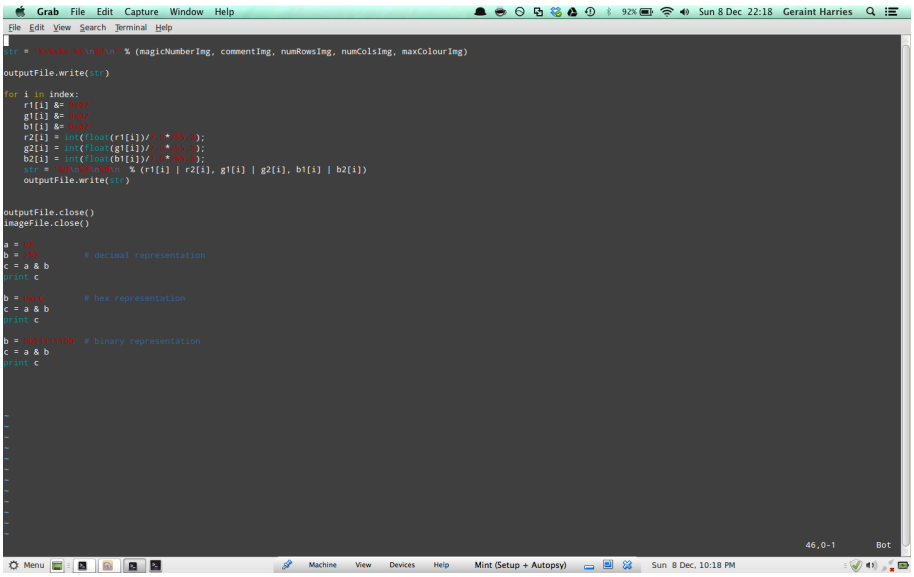

Figure 6: _nake Page 2

Figure 7: _ombined.png

Figure 8: _ombined.ppm

Figure 9: AngleFish.ppm

Figure 10: AngleFish.png

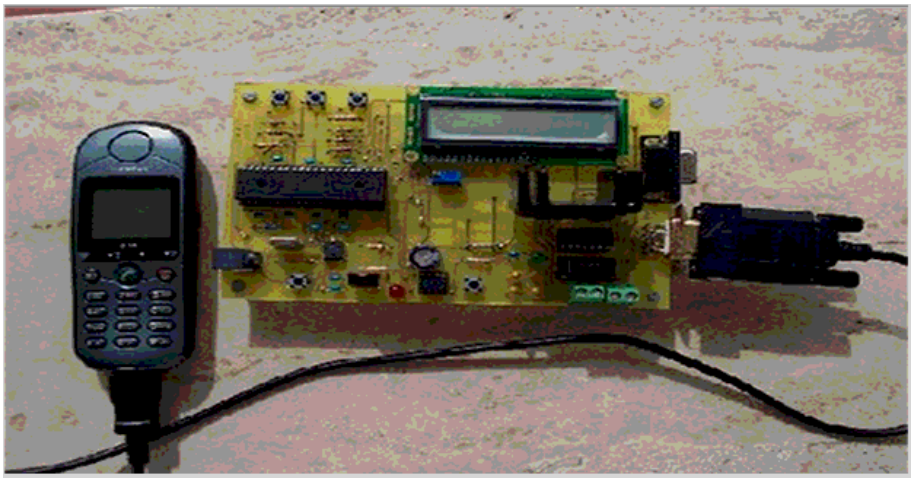

Figure 11: This image was generated by running AngleFish.ppm through the _nake.py script