EXAMPLE OF AN EXPERT WITNESS DIGITAL FORENSIC REPORT

By: Vincenzo Crawford

BS. FORENSIC SCIENCE, University of Technology (U-Tech), Jamaica

INVESTIGATOR:	**Patrick Linton**
	CEO
	Digital Inc.
DIGITAL FORENSICS EXAMINER:	**Vincenzo Crawford**
	Detective #1005315
	Faculty of Science and Sports (FOSS), Digital Forensics Expert
	Portmore, St. Catherine
	(876) 782-0696
SUBJECT:	**Digital Forensics Examination Report**
OFFENCE:	Money Laundering, Embezzlement, Insider Trading, Scamming, Racketeering activities, Fraud,Terrorism and Forgery
ACCUSED:	**Therese Brainchild**
DATE OF REQUEST	Oct. 27, 2013
DATE OF CONCLUSION	Nov. 09, 2013

Contents Page

Background to the case

Questions asked relevant to the case 1

Search and seizer and transport of evidence 2

- Exhibits submitted for analysis
- Further Questions Asked Relative To The Case

List of Criminal Offence 3

Evidence to Search For 4

Deleted files of evidentiary value to the case 5

Corporate Breach 6

Examination Details 7

Deleted, Encrypted and Steganographic files 8

Analysis Results 9

Conclusion 10

General Material 11

Background to the Case

Therese Brain child, a master accountant hired by Safe Data Associates was suspected of being engaged in cyber crimes, industrial espionage, embezzlement and terrorism. The aid of Digital forensics along with legal authorities was employed by Patrick Linton's Digital Inc. in order to exonerate or convict the accused (Therese Brainchild). Brainchild opted to delete files from her thumb drive kept at her workstation before being escorted from the building and her administrative duties. She swears she is innocent of all accusations, However, intelligence shows that in 2008, Therese Brainchild converted J$30M of criminal proceedings to start a construction business in order to legitimize her illicit earnings.

To conduct an effective and efficient investigation, I employed the use of the Forensic Tool Kit Imager software (FTK Imager) in order to recover the files deleted from the thumb drive said to be that of Brainchild's;
Based on my expert knowledge of digital forensics, these deleted files will still be lingering in what is called the 'unallocated space' of the thumb drive.

1. Questions Asked Relevant To The Case

Further background Checks were conducted on Brainchild. She was questioned in order to acquire legitimacy for data acquisition. The following questions were brought forward:

	Questions
1.	Is the computer system, thumb drive and other devices personal or were they assigned to Brainchild by the company?
2.	Does anyone else in or out of the company have any form of access to these devices or to the assigned workstation of Brainchild's?
3.	If these devices were assigned by the company, were they being used before, during and or shortly after they were assigned to the accused (Therese Brainchild)?

2. Search and seizer and transport of evidence

A request was filed for legal authorities to enter the dwelling of Theresa Brainchild. The warrant was issued for the search and seizer of devices which may be analyzed and serve as digital evidence, in order to convict or exonerate her. Upon the search and seizer of the necessary devices which may provide digital evidence, the acquired materials were carefully package and a chain of custody was efficiently established; so to ensure the integrity of the evidence.

Exhibits Submitted for Analysis

Cons#	Exhibits Description and Model	Serial number
1.	Burgundy Wi-Fi Mobile Cellphone	355600084947547
2.	Nokia Mobile Phone	359831087172837
3.	Grey and Silver Kingston Thumb drive	F13225YY
4.	Black and Grey Compaq Presario C600 laptop	CND6752RJN
5.	Black Dapeng cellphone	358729025499270

	Further Questions Asked Relative To The Case
4.	Were the three(3) cell phones; exhibits 1, 2 and 4 [serial- (355600084947547), (359831087172837) and (358729025499270), respectively] used to call individuals, or browse for information which may be deemed as incriminating and of relevance to the investigation?
5.	Did anyone else other than the accused have access to the thumb drive; exhibit 3 [serial-(F13225YY)] before, during and or after Brainchild's possession of it?

3. Evidence to Search For

Based on the nature of the case and all that which have been made against the accused (Therese Brainchild), to begin analysis of the obtained evidence, the search for data of probative value to the investigation will be in the area of; (A) acquiring the browsing data from the laptop and cell phones' browsers, (B) investigate the previous locations and calls made to and from the cell phones, (C) The acquisition of files deleted from the laptop, phone memories and most importantly files deleted from the thumb drive.

4. List of Criminal Offence

The criminal offences facing 'Therese Brainchild' are; money laundering, embezzlement, terrorism, Racketeering Activities, Insider Trading/ industrial espionage, fraud, forgery and scamming.

5.	**Deleted files of evidentiary value to the case**
5.1	Three (3) folders containing files of probative interest to this investigation were recovered from the Grey and Silver Kingston Thumb drive bearing the serial number F13225YY. These documents contained; code clues, encrypted and steganographic files, erroneous documents, stolen credit cards information, cheque details, information on lottery winners.
5.2	From the documents acquired, the files contained; bank account details of Therese Brainchild, names, address, telephone numbers and credit card numbers of persons who might have won the lottery, along with employees' information of the company which she was hired.
5.3	Five (5) notepad files disguised by the steganographic techniques were uncovered from the thumb drive of Therese Brainchild. The five (5) txt files recovered contained names, address, phone numbers and credit card information of individuals. Among these files, were steganographic clues to encrypted data.
5.5	Two (2) Microsoft excel documents were recovered; the first excel document identifying that files were copied and transferred to another company, and the second excel document containing Therese Brainchild's personal account number (43524324-234234324324).
5.6	Five (5) Microsoft word documents were recovered, containing Therese Brainchild Swiss bank account number (4332432432-4324324324324-234324423), Transaction information, and contractual/lottery forms.
5.7	Twenty four (25) photo files were recovered, some of which were steganographic files. However, only 4 of these documents were relevant to the investigation as they contained, lottery leads, bank cheque, stolen credit cards information and a terrorist map.
5.8	One (1) Microsoft access (Database) document was found containing customer and employees' detailed information (names, positions, ID numbers, bill payments and account numbers, accounts above 3000 dollars).

6. Corporate Breach

Theresa Brainchild, deemed to have committed corporate breaches such as; the breach of contract to maintain data integrity and company confidentiality, falsification of data, Embezzlement and industrial espionage.

7. Examination Details

I employed the use of FTK imaging technique in order to recover the deleted files from the Grey and Silver Kingston Thumb drive (serial# F13225YY) confiscated from the accused (Therese Brainchild). The sha1 hash value (904e2abcf6f559e70bd9e6516ef3429dd) and MD5 hash value (3b50d4fd1421e5c5c29e3345f7fd0561bc1d5370) were obtained in order to aid in proving the legitimacy of the files recovered. Among the files recovered, there was a database document named 'Snowden Employee.mdb', containing the following information; (i) customers' names and account numbers, (ii) Employees' names, ID numbers and address, (iii) Quarterly bill cycle and Employee accounts below and 'above $3000'.

7.1 Sha1 and MD5 hash value for all documents and deleted files obtained from Brainchild's Thumb drive [serial- F13225YY] via FTK imager.

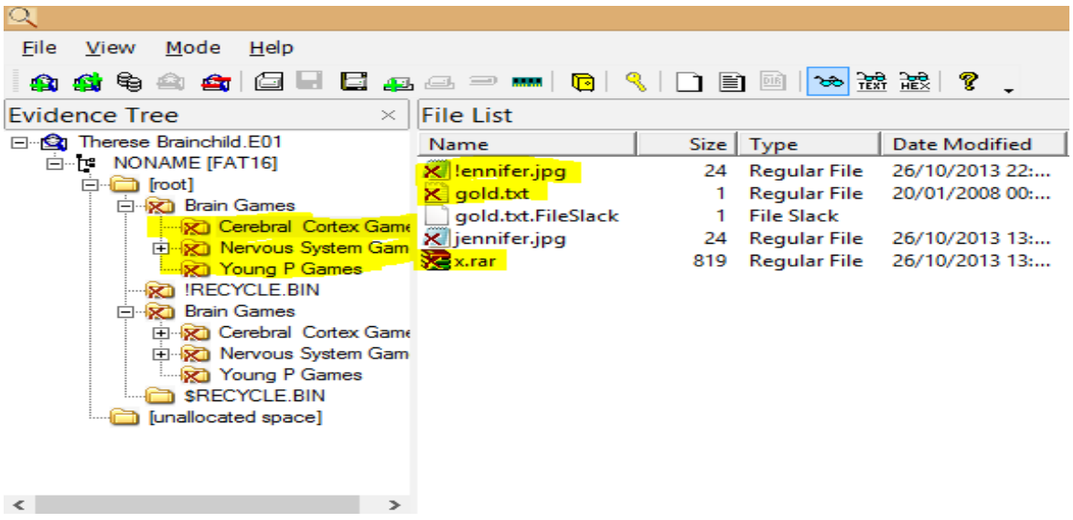
MD5	SHA1
4516bc7e2b2f68b8dcf3fbc1a256256e	1d899c89e8224b022ed9cb3619d036ea08195bf6
422e327a54b49e2bc50f0ef3dd218795	ce75b695ae3e78bd78f1fbe41d21da895823c077
bccb74803cdad52a4f0eadec92403e4a	7f4f6ea48edf0bb8722b4a68b499293216f0887b
5e2b09eb0b05d9e124613eb1ffac27ee	0132d6aa5a581a179c16fe19bedf426a77031120
d0db850ad982b1640182acec9b75aa35	3606629d1f8d3314832423ba101c3f08d14834b2
421c6a356358ca20ef750e7cbb04c140	49b48ab09d0f2542a7f0012542c530c36ded7caf
1be6c5be960851477469fca61e86dc3f	8f2074940ee5056a8ecafebf2a28bd1d055fe702
4418fe61f16bebf1dd7b22d7d1a67a9e	0184a98c612f235d32f8053b5d47eefc6f65ada9
bec831382b2c37f09f115e23d3067afa	1df94e0d71ba9d30c77c821abb674f48167b60e8
718ba18fd768df5f814d1d12ec3d9d4b	8f51fac1b506936523be5143c66fc34b379eb506
b4b9e59b1ca6d9ae04bf5f45127e52af	916c05d397b36761bc016b080b76c57fe0420906
bacadf3e9df696f96446db014295e8d8	d39aff4ea5061e52e9fa4f6142700fc9ae02738d
55496c77e2c0532c0310c69dadd30f21	a8b566da5d9142a33da1cdae3b67b064dd016eaf
0b9a0f3d3b36af6f38762cc9544e92a0	97cd0235451ee6a32e4602973ac41c756b7d291e
2d5255508134339804177c037cf086b8	c93fdec71dea265093d8311146babc286dcb9fc8
eb8731db825e01260761fed95d16c77a	3b049f654804ba89d3d976f7bf99e8c8f627b276
9d8f063b3cfaca03b0be7b3c39fc09b8	39a9446af56fccd92d65ffe3852bbd49b613847d
f5aa1d1da28224ee0dd8e55fc40bcc53	029643f9c426a1d396372398874f4cdd3b4f745d
3470d5c0746deeb68484c8fd69225a8a	4be2d7b990714f574923c8d355c381d9d7536382
34956da8ec293972513ba1d0943d4479	e6e15f29daeca48003ccbc448a256053bd674198
d34d89cd328f6edd410273988d68a483	d39c90a5d1017097069f327f93db2c77b4d3e76c
e27938ff3830fa6ed5a4bc0775484fb2	3d0091bceb32bb0f99090407d36d968e28a2b59b
0fa71c70567d26092615435c86830827	b9509292fd0f1cd08ab7725bc854c9f81eb319da
ef0bd6deb4f04e241eefff19e80cc82d	851026c80bb1122c6b9d2094447d90e05e185cc3
b5f45ed1c3f331df2962005f485bfa48	ec870d4cab1800a707028596bfdb488927bde6e9
4d24b2f799fe007239df880ec3aaf051	78767a5c3978b8c266ea1eda98221e572f2ff3cb
12f1e05d2bc553bf981721229818e6ec	d936bb81ef45b1e03aa71040c9a11e1d94c0010f

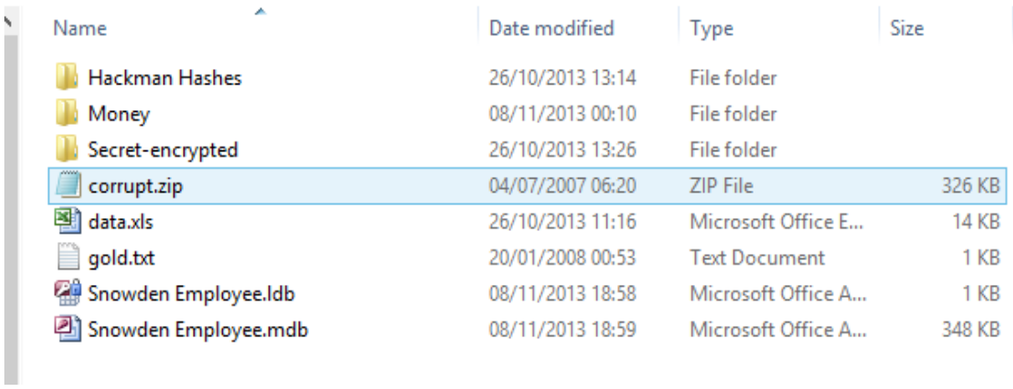
8. Deleted, Encrypted and Steganographic files

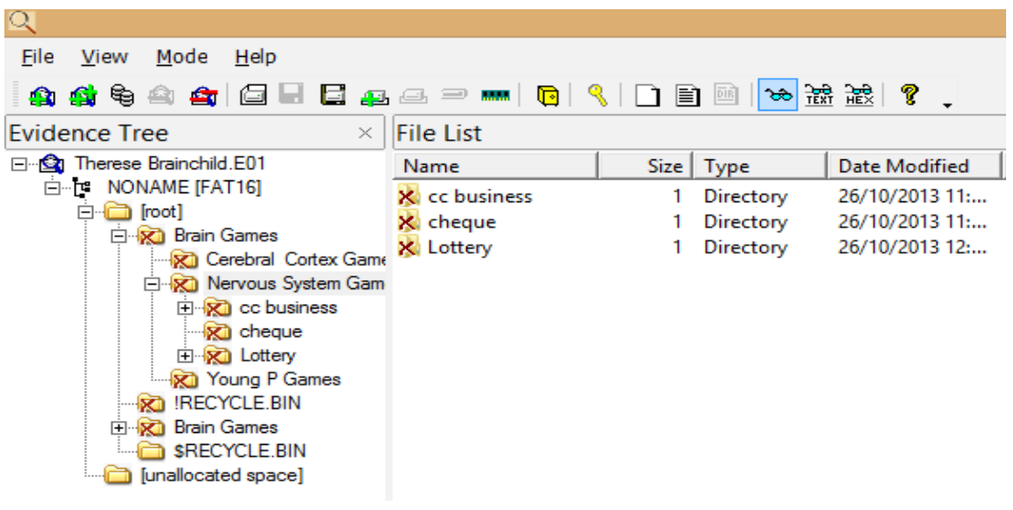
Approximately forty-one (41) files of different formats were deleted. Of all the files retrieved, two (2) files and one (1) folder was encrypted. The encrypted files were cracked as a result of steganograpic files which contained clues and passwords to break the encryption. The encrypted files and passwords are as follows; .Rar file entitled 'x' containing; 1) Database documents of customer and employees' detailed information (names, positions, ID numbers, bill payments and account numbers, accounts

above 3000 dollars). 2) A Microsoft Excel file entitled 'MONEY' containing a Microsoft Excel document with the accused personal bank account number. 3) A Microsoft Word file entitles 'SECRET-ENCRYPTED' containing the accused Swiss bank account number.

The steganographic files obtained were hidden in various forms (.txt .jpg .zip etc). All steganographic files were recovered and are as follows: (1) The Password [alpha] for Therese Brainchild's personal account was hidden in what APPEARED to be an .mp3 file named ' me.mp3'. (2) The Password [love] for Brainchild's Swiss bank account was hidden in what APPEARED to be a .jpg file named ' sample.jpg'. (3) A file entitled 'corrupt' which APPEARED to be a .zip folder, contained a picture of a map. (5) The hackman hash files containing random pictures (irrelevant to the investigation).
The Personal and Swiss bank account numbers of Therese Brainchild recovered from encryption is; [(43524324-234234324324) and (4332432432-4324324324324-234324423) respectively]. separate and aside from the bank account numbers were the terrorist map which was hidden in the file entitled 'corrupt' which APPEARED to be zip folder.







9. Analysis Results

From the above exhibits;
The cell phones confiscated for analysis, 'Burgundy Wi-Fi Mobile Cellphone', 'Nokia Mobile Phone' and 'Black Dapeng cellphone', exhibits 1, 2 and 5 [serial- (355600084947547), (359831087172837) and (358729025499270), respectively], were analyzed and I calculated their check digit in order to verify the IMEIs which intern reveals the make, model, date and country of origin of all three exhibits.

The check digits calculated are as follows:
Exhibit 1, Wi-Fi Mobile Cellphone, [serial - 355600084947547, corrected was found to be '6'].
Exhibit 2, Nokia Mobile Phone, [serial - 359831087172837, correct check digit found to be '4'].
Exhibit 5, Black Dapeng cellphone, [serial - 358729025499270, [check digit remains unchanged '0']
Further analysis brought to the forefront, identified metadata information which proved to be vital to this investigation. Password clue to the binary digits password [10101111] required to open the 'rar' file entitled 'x' containing fraudulent activities of Therese Brainchild. Passwords were also hidden in Steganography files which lead to brainchild's Personal bank account and Swiss bank account.

10. Conclusion

- The recovery of all data of evidentiary relevance to the investigation was made possible, and I managed to maintain the integrity of all the deleted data during its recovery as all the exhibits were protected and verified by checking hash values and recalculating check digits during the examination.
- I was able to recognize lottery related documents and leads lists, pitch documents, cheques and other documents pointing to fraudulent activities
- The digital devices analyzed showed many involvement of illegal activities.

11. Generated Material

- Microsoft word document of Digital Forensic Report and Findings
- Evidence found on Exhibits