***DIGITAL FORENSIC INVESTIGATION REPORT***

***REQUESTED BY:*** *DR. VIRGINIA FRANQUEIRA*

*UNIVERSITY OF DERBY*

***DATE****: 20ST April, 2016*

***CASE****: DIGITAL FORENSIC INVESTIGATION OF THE EVIDENCE AQUIRED FROM THE DEFENDANT MR. SAM MALONE BEING INVESTIGATED FOR ILLEGAL WIRE TRANSFERS AND ILLEGAL WEAPON TRADING*

***CASE NUMBER****: Malone\_2016\_Derby*

***CLAIMANT:*** *UNIVERSITY OF DERBY*

***DEFENDANT:*** *MR SAM MALONE*

***INVESTIGATOR:*** *MR. BADE-ADEBOWALE KEHINDE*

*UNIVERSITY OF DERBY*

*KEDLESTON ROAD DERBY*

*DE22 1GB*

***TELEPHONE NUMBER****: 07543160269*

***EMAIL****:* [*k.badeadebowale1@unimail.derby.ac.uk*](mailto:k.badeadebowale1@unimail.derby.ac.uk)

Contents

[SUMMARY OF CONCLUSSION 3](#_Toc449021744)

[1 INTRODUCTION 3](#_Toc449021745)

[1.1 BRIEF CURRICULUM VITAE 3](#_Toc449021746)

[1.2 INSTRUCTIONS 3](#_Toc449021747)

[1.3 BACKGROUND OF CASE 3](#_Toc449021748)

[1.4 INVOLVED PARTIES 3](#_Toc449021749)

[2 ISSUES 4](#_Toc449021750)

[2.1 REPORT REQUIREMENTS 4](#_Toc449021751)

[2.2 CHALLENGES 4](#_Toc449021752)

[3 TOOLS 4](#_Toc449021753)

[4 METHODOLOGY: APPLYING THE CFSAP MODEL 4](#_Toc449021754)

[5 INVESTIGATION 5](#_Toc449021755)

[5.1 SECURING & PRESERVATION OF EVIDENCE 5](#_Toc449021756)

[5.2 ANALYSIS OF EVIDENCE 6](#_Toc449021757)

[6 OPINION 10](#_Toc449021758)

[REFERENCES 11](#_Toc449021759)

[EXPERT’S DECLARATION 12](#_Toc449021760)

[STATEMENT OF TRUTH 13](#_Toc449021761)

[APPENDICES 14](#_Toc449021762)

[APPENDIX 1 CV 14](#_Toc449021763)

[APPENDIX 2 BITLOCKER 15](#_Toc449021764)

[APPENDIX 3 TIME ZONE 16](#_Toc449021765)

[APPENDIX 4 DISK ANALYSIS 17](#_Toc449021766)

[APPENDIX 5 EVIDENCE PROCESSING 19](#_Toc449021767)

[APPENDIX 6 EMAIL CONVERSATIONS & DOCUMENTS 20](#_Toc449021768)

[APPENDIX 7 ANALYSIS OF THE E DRIVE 27](#_Toc449021769)

[APPENDIX 8 GLOSSARY 30](#_Toc449021770)

# SUMMARY OF CONCLUSSION

*After careful and detailed digital forensics investigation of the* ***image file*** *(See section 1.3, item i), from my expert stand point I can deduce that there were activities of illegal trade of weapons and illegal wire transfer of funds to offshore accounts after carefully.*

# 1 INTRODUCTION

## 1.1 BRIEF CURRICULUM VITAE

*Mr. Bade-Adebowale Kehinde K. has a B.Tech. In Computer Science from the Bells University of Technology, a Postgraduate certificate in Information Security Management from Fanshawe College London ON., a Postgraduate certificate in Object Oriented Software Development from Southern Alberta Institute of Technology Calgary AB., and is currently a student of the MSc of Digital Forensics and Compute Security of the University of Derby.*

*Please refer to Appendix1 for extensive CV.*

## INSTRUCTIONS

*Conduct a digital forensic investigation of the evidence file “Malone’s HDD 1A.E01” in the criminal case of Mr. Sam Malone to find out activities of:*

1. *Illegal wire transfers to off-shore institutions*
2. *Illegal trade of weapons*
3. *Activities aiding i. and ii.*

## 1.3 BACKGROUND OF CASE

*On the 19th of January 2016, the University of Derby made available to me:*

1. **image file**: *Malone’s HDD 1A*.E01
2. email address: [smalone1993@gmail.com](mailto:smalone1993@gmail.com)

*These belongs to the defendant Mr. Sam Malone who is being investigated for alleged involvement in illegal wire transfers and illegal weapons trading.*

## 1.4 INVOLVED PARTIES

*Parties in this case are:*

* + *The Claimant - The University of Derby*
  + *The Defendant - Mr. Sam Malone*
  + *Instructor - Dr. Virginia Franqueira*

# 2 ISSUES

2.1 REPORT REQUIREMENTS

*This report is required to explicitly carry out a digital forensic investigation of the defendant’s* ***image file*** *(See section 1.3, item i) and get evidence that shows the defendant’s involvement in 1.2 i, 1.2 ii and 1.2 iii.*

## 2.2 CHALLENGES

*There was only one evidence provided for this forensics investigation which is the* ***image file*** *(See section 1.3, item i) acquired from the defendant (See section 4.1, item i). Furthermore the content of the file “deal.jpg” and “OWAT Software for al qaeda” could not be read because it was encrypted with a software called “truecrypt” which I could not get the key needed to decrypt it (See Appendix 6, item viii). If I had access to more digital evidence’s and the encrypted files, I would have been able to have a better understanding of the gravity of the defendant’s activities.*

# 3 TOOLS

*The following are the tools used at any time during the investigation of this case by me:*

* Guidance® Software's EnCase Version: 7.11.01.05 ®
* OneNote Version: 16.0.6741.2021
* Adobe Acrobat Pro DC Version 2015.007.20033
* Microsoft Word Version: 16.0.6741.2021
* Google Chrome Version 49.0.2623.112 m
* Power Point Version: 16.0.6741.2021

# 4 METHODOLOGY: APPLYING THE CFSAP MODEL

*A model that integrates the four major segments of digital forensics investigation i.e. Identification, preservation, analysis and presentation will be adopted. Taking that into consideration, the Computer forensic-secure, analyse, present model (CFSAP) (Mohay, 2003) will be adopted throughout this investigation. It converts the four major segments into three segments i.e. Secure Analyse and Prepare (See Figure 4).*

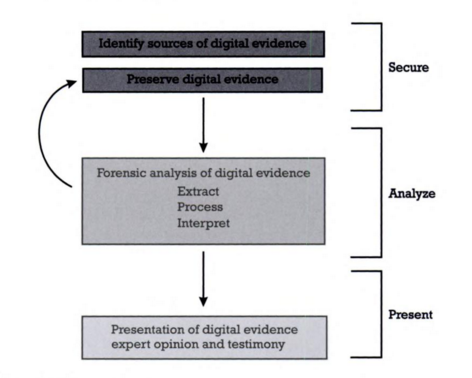


Figure 4 The CFSAP model (Mohay, 2003)

# 5 INVESTIGATION

*I will follow the ACPO good practice guide for digital evidence (ACPO, 2012) while using the CFSAP methodology (See Figure 4).*

## 5.1 SECURING & PRESERVATION OF EVIDENCE

*This stage contains the* ***identification*** *and* ***preservation*** *of digital evidence. I skipped the* ***identification*** *stage because the evidence file was not acquired by me (Please see chain of custody document).*

*The evidence* ***preservation*** *was done by storing the* ***image file*** *in a write-proof location so that the contents of the file cannot be altered (See Figure 5.1, item i)*

* *File* ***path****:* *S:\Common Area\Forensics - All Years\Evidence Files\Malone*

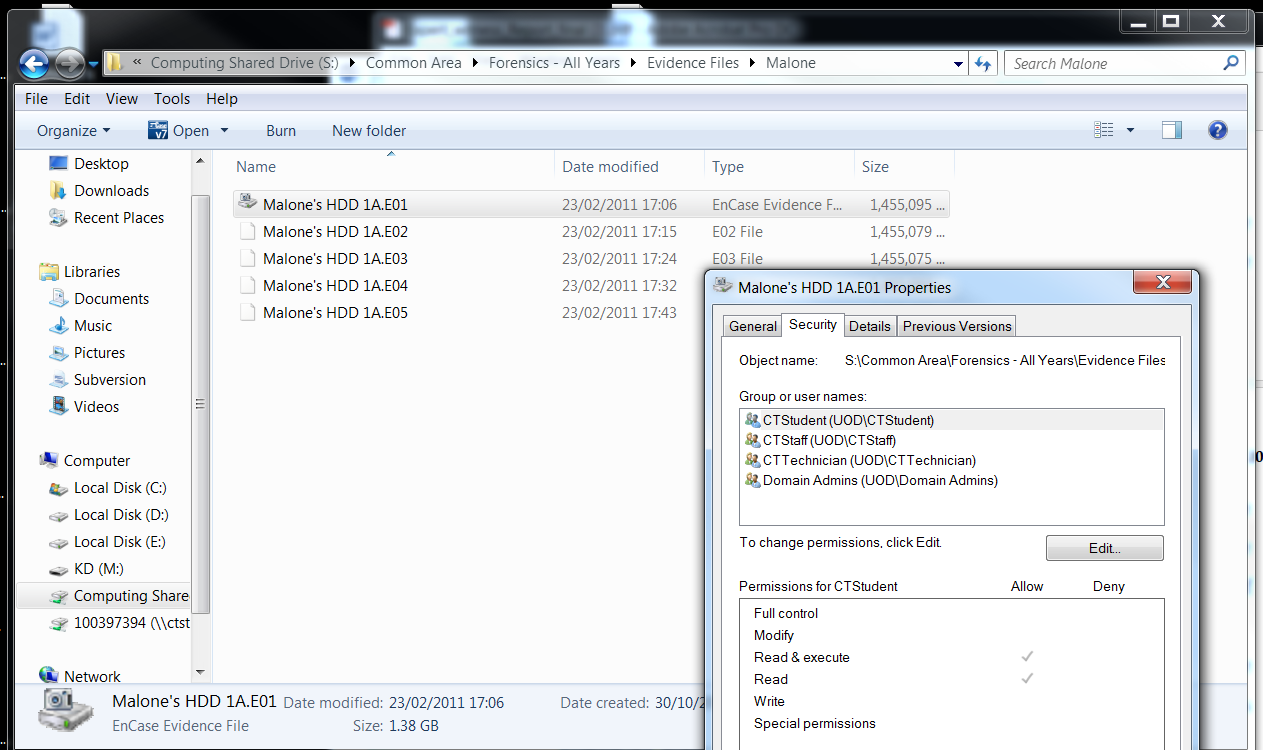


Figure 5.1-i stored location of the evidence file showing it is write-proof

## 5.2 ANALYSIS OF EVIDENCE

***VERIFICATION****: The* ***image file*** *was extracted using EnCase after which EnCase started verifying the* ***image file****. This is done by comparing the* ***verification*** *and Acquisition MD5 and SHA1 hashes to make sure that the* ***image file*** *has not been altered to maintain the integrity of the* ***image file****. The hashes are:*

* *Acquisition MD5: 73d8ca8c90ff775237e0c962444bf87e*
* *Verification MD5: 73d8ca8c90ff775237e0c962444bf87e*
* *Acquisition SHA1: 677dbe7978f11a412040de1ec386b6594723bb2f*
* *Verification SHA1: 677dbe7978f11a412040de1ec364b6594723bb2f*

*(See Figure 5.2, item i)*

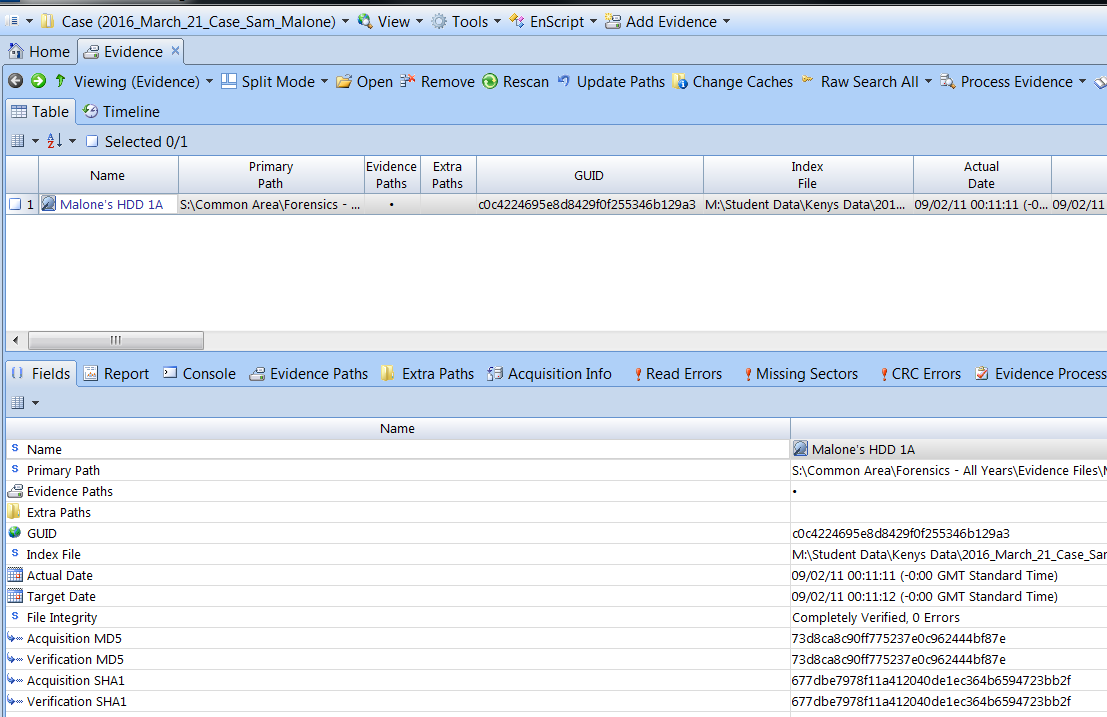


Figure 5.2-i Evidence Verification=

***BITLOCKER****: After the* ***verification*** *is done I opened the* ***image file*** *and found out it was BitLocker encrypted. This made me do a raw search for the recovery key using the following keywords:*

* ***BitLocker***
* *Recovery Key*
* *Password*

*After the search I recovered the key and decrypted the disk using the* ***BitLocker*** *recovery key (See Figure 5.2-ii)*

* *Recovery Key Identification: 6C894E50-13B4-48*
* *Full recovery key identification: 6C894E50-13B4-48DC-AAD3-3FFAD5C9A271*
* ***BitLocker*** *Recovery Key: 447744-331595-256102-506561-409002-304843-145365-165000*

*(See Appendix 2)*

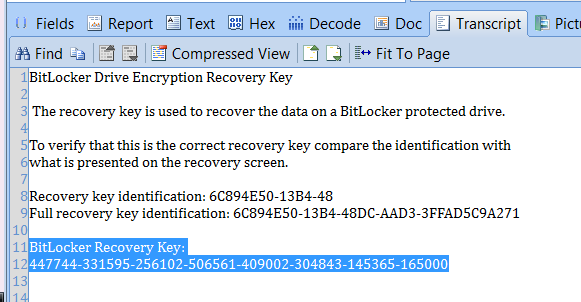


Figure 5.2-ii BitLocker Key

**TIME ZONE CONFIGURATION:** *I checked the time zone settings of* ***image file*** *on* ***acquisition*** *and discovered it is Pacific Standard Time (PST) (See Figure 4.2, item iii). After this discovery I changed the time zone of my working environment to Pacific Standard Time (PST). The file* ***path*** *indicating the time zone on acquisition is:*

* ***Path****: C/Windows/System32/config/SYSTEM*

*(See Appendix 3 for the true path)*

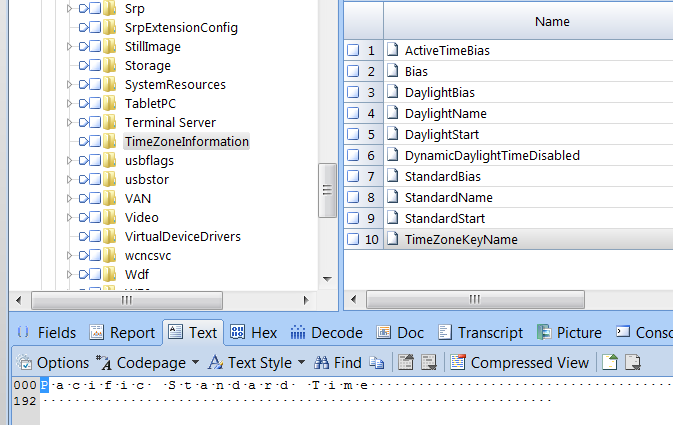


Figure 4.2-iii The TimeZoneInformation folder containing the TimeZoneKeyName notifying us of the Time zone of Acquisition

***DISK ANALYSIS:*** *A deleted FAT32 partition was discovered while analysing the disk. (See Table 1). The deleted FAT32 partition with Master Boot Record at sector 39843840 was recovered (See Appendix 4).*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Partition* | | | | |
| *Name* | *Type* | *Size of Partition* | *Start (MBR)* | *End* |
| *C* | *NTFS* | 39,842,791 | *2,048* | *39,843,839* |
| E | FAT32 | 819,200 | *39,843,840* | 40,663,039 |
| D | NTFS | 1,275,903 | 40,663,040 | 41,938,943 |

*Table 1 – MBR, sector locations and name of the partitions*

***EVIDENCE PROCESSING:***  *The evidence was processed for Files and Folder Recovery, File signatures analysis, secured files analysis, Compound files expansion, Email analysis, and Locating internet artefacts (See Appendix 5).*

***ANALYSIS OF EMAIL:***  *The following were discovered after the analysis of the email conversations on the* ***image file:***

* *Mr. Sam Malone acquired from Mr. Cliff Cavin the following*
  + *Ordinance and Weapons Acquisition Tracking software (OWAT)*
  + *Predator type drones support and upgrades.*
* *Payment was made by Mr Sam Malone Acquired to Mr. Cliff Cavin*
  + *Amount: $22,950,000,000.00*
  + *Account Number: 89-2384993947*
  + *Bank Name: Bank of Antigua*
* *Series of conversation between:*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Parties*** | ***Name*** | ***Email*** | ***Time Frame*** |
| *Defendant* | *Mr. Sam Malone* | [***smalone1993@gmail.com***](mailto:smalone1993@gmail.com) | *29/01/11 18:38:14 (PST)* |
| *Seller* | *Mr. Cliff Cavin* | [***cliffcavin39@gmail.com***](mailto:cliffcavin39@gmail.com) | *07/02/11 16:31:05 (PST)* |

*Table 2 – Email of the defendant and the time frame of the conversation between his email and Mr. Cliff Cavin*

(*See Appendix 6 for more information).*

***INTERNET ARTEFACT ANALYSIS:*** *The following was discovered after carefully analysing the internet artefacts of the* ***image file:***

* *There are frequent searches for pictures relating to explosions (See figure 4.2, item iv)*
* *There are also frequent visits to* [*www.t0.gstatic.com*](http://www.t0.gstatic.com) *a website that houses several pictures of explosions.*
* *Two visits to* [*www.truycrypt*](http://www.truycrypt) *Site used for the software encryption (See figure 4.2, item v)*

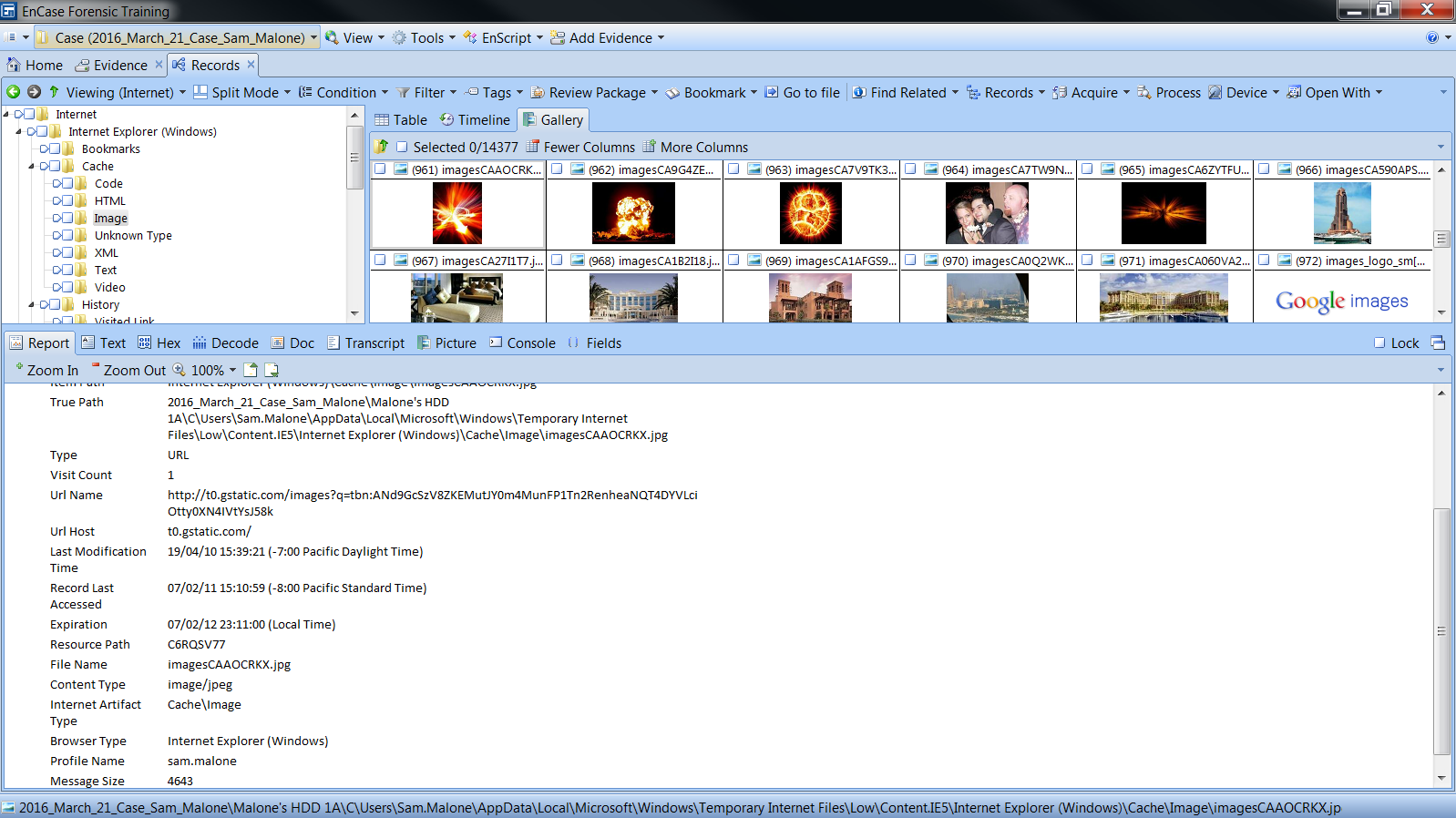


Figure 4.2-iv – Frequent searches for pictures of explosions

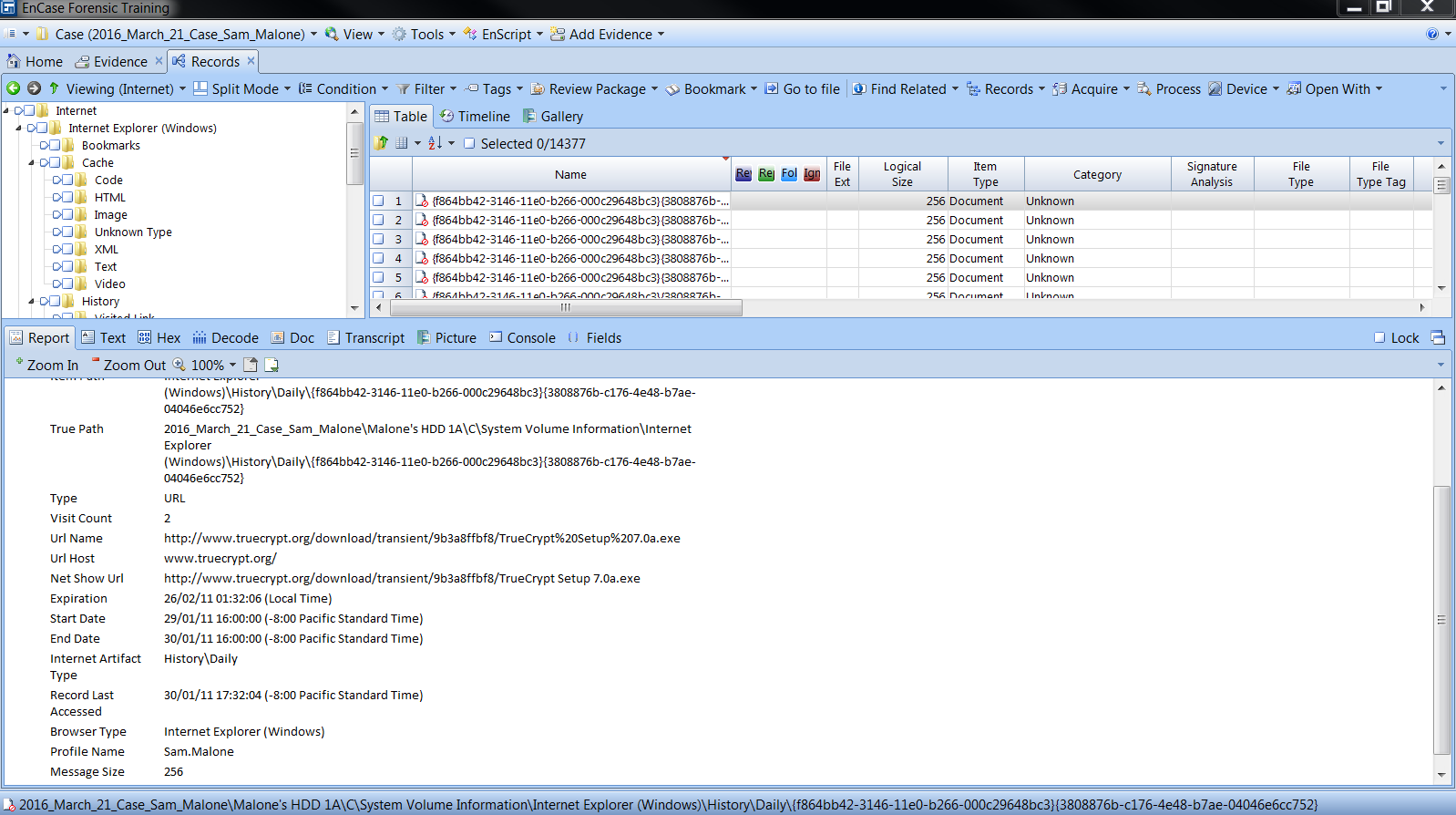


Figure 5.2.v two visits to truecrypt the website used for encryption

***ANALYSIS OF THE E PARTITION:*** *I have to do a special analysis of the E partition because it was deleted from the filesystem. The questions asked regarding the partition being deleted warranted this special analysis. After the careful analysis of the E partition, I discovered the following:*

* *Suspicious folders in the E drive (See figure 5.2, item vi)*
* *Received $1,550,999,000.00 from terrorist organization Al Qaeda in total*
* *Frequent travels to the middle east*
* *Encrypted folder called “OWAT Software for al qaeda”, which suggests that the OWAT software is accessible by the terrorist organization*
* *Statement of account indicating huge transfer of funds through third parties*

*(See Appendix 7)*

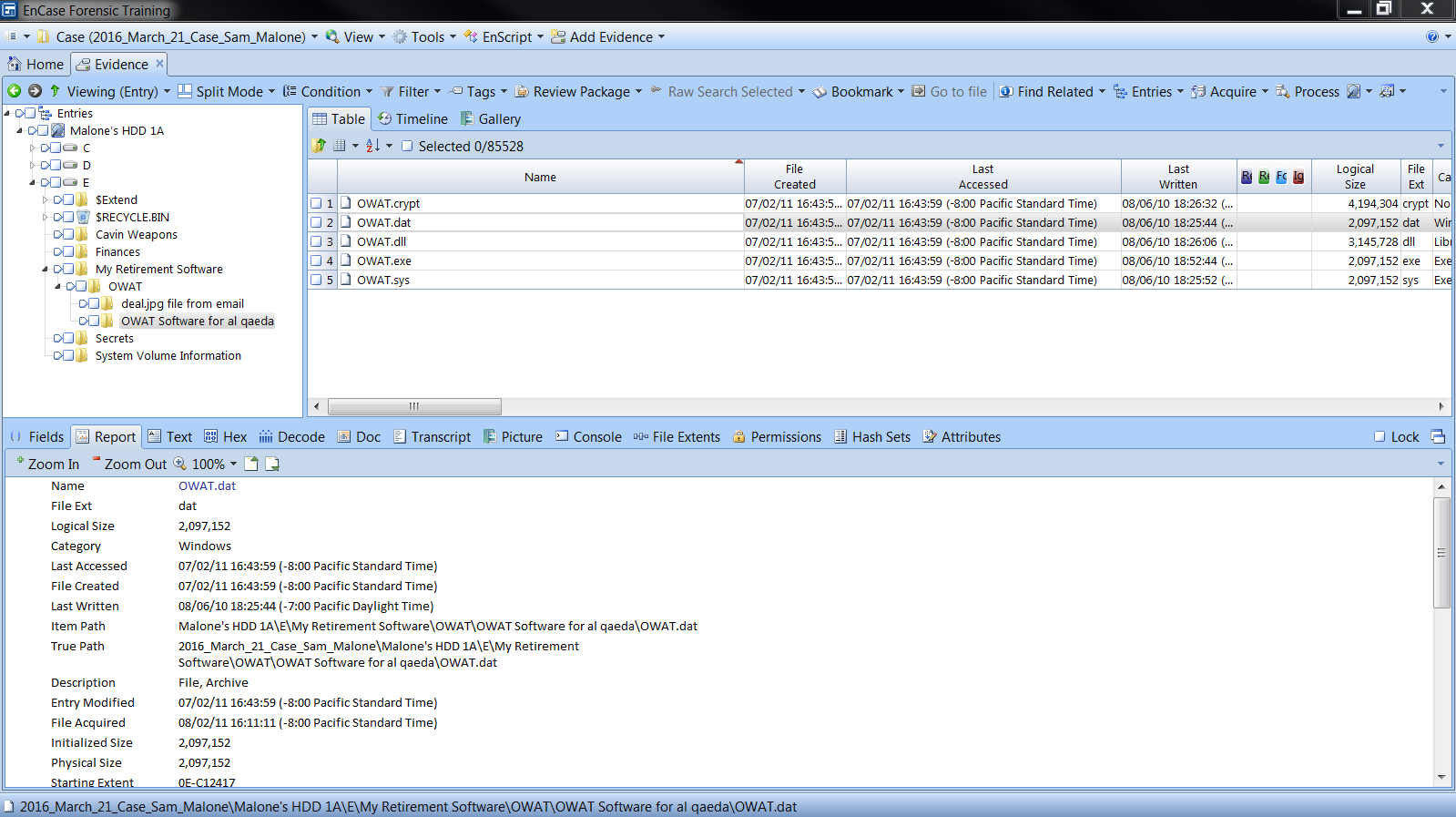


Figure- 5.2-vi suspicious folders in the E drive

# 6 EXPERT OPINION

*Payments were made for an “Ordinance and Weapons Acquisition Tracking Software (OWAT)” into Mr. Cliff Cavin’s company account which violates the United States International Traffic in Arms Regulations if the defendant does not possess licence to trade arms.*

*There was an encrypted folder called “OWAT Software for al qaeda” (name of a terrorist organization) suggesting information secretive to Mr. Sam Malone with regards to his dealings with this organization and Mr. Sam Malone received as much as $1,550,999,000.00 from the terrorist organization (Al Qaeda) which is Money Laundering as defined by the USA Patriot Act (Patriot Act, 2001) and the EU Payments Regulation as Money used to fund terrorism (Gov.uk, 2014).*

*Mr Sam Malone’s account was also used to transfer huge amount of funds into different countries. Some of the funds that raised flags are:*

* *A deposit of $775,000.00 into BoA MM*
* *A deposit of $4,289,000.00 Bank of Lativa*
* *A deposit of $925,000.00 into Bank of Investment*
* *A deposit of $6,998,050.00 into Citizens Bank of Costa Rica*
* *A deposit of $17,980,400.00 into Prime Investments of Spain*
* *A deposit of $87,900,500.00**into Prime Investments of Spain*
* *A deposit of $87,900,500.00**into Prime Investments of Spain*

*The purposes of these transactions could not be confirmed at the end of the investigation, but some other transactions were like the $450,000,000.00 for the purchase of hundred predators which is also Money Laundering as defined by the USA Patriot Act (Patriot Act, 2001) and the EU Payments Regulation as Money used to fund terrorism (Gov.uk, 2014) if the defendant does not have the proper licencing to do so.*

# REFERENCES

*NIST SP 800‐86 (2006).  Guide to Integrating Forensic Techniques into Incident Response.* [*http://csrc.nist.gov/publications/nistpubs/800‐86/SP800‐86.pdf*](http://csrc.nist.gov/publications/nistpubs/800‐86/SP800‐86.pdf)

*Mohay, G. (2003). Computer and intrusion forensics. Boston: Artech House.*

*Gov.uk. (2014). Money Laundering Regulations: introduction - Detailed guidance* [*https://www.gov.uk/guidance/money-laundering-regulations-introduction*](https://www.gov.uk/guidance/money-laundering-regulations-introduction)

*Congress.Gov. (2001). USA Patriot Act of 2001.* [*https://www.congress.gov/bill/107th-congress/house-bill/3162*](https://www.congress.gov/bill/107th-congress/house-bill/3162)

*Casey, E. (2004). Digital evidence and computer crime. London: Academic Press.*

*ACPO (2012). 4th ed. [ebook] UK: 7Safe, pp.3-34. Available at:* [*https://www.cps.gov.uk/legal/assets/uploads/files/ACPO\_guidelines\_computer\_evidence[1].pdf*](https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5b1%5d.pdf) *[Accessed 21 Apr. 2016].*

# EXPERT’S DECLARATION

*Individual items of the Experts’ Declaration may have to be varied or omitted, depending on the circumstances of the particular report. Although not required by the Practice Direction it could also be useful to confirm that the report has been prepared in accordance with the Code of Guidance on Expert Evidence.*

1. I understand that my overriding duty is to the court, both in preparing reports and in giving oral evidence. I have complied and will continue to comply with that duty.
2. I have set out in my report what I understand from those instructing me to be the questions in respect of which my opinion as an expert are required.
3. I have done my best, in preparing this report, to be accurate and complete. I have mentioned all matters which I regard as relevant to the opinions I have expressed. All of the matters on which I have expressed an opinion lie within my field of expertise.
4. I have drawn to the attention of the court all matters, of which I am aware, which might adversely affect my opinion.
5. Wherever I have no personal knowledge, I have indicated the source of factual information.
6. I have not included anything in this report which has been suggested to me by anyone, including the lawyers instructing me, without forming my own independent view of the matter.
7. Where, in my view, there is a range of reasonable opinion, I have indicated the extent of that range in the report.
8. At the time of signing the report I consider it to be complete and accurate. I will notify those instructing me if, for any reason, I subsequently consider that the report requires any correction or qualification.
9. I understand that this report will be the evidence that I will give under oath, subject to any correction or qualification I may make before swearing to its veracity.
10. I have attached to this report a statement setting out the substance of all facts and instructions given to me which are material to the opinions expressed in this report or upon which those opinions are based.

# STATEMENT OF TRUTH

I confirm that insofar as the facts stated in my report are within my own knowledge I have made clear which they are and I believe them to be true, and the opinions I have expressed represent my true and complete professional opinion.

**Signature**: ­*BADE-ADEBOWALE KEHINDE*  **Date:** 21ST April, 2016

# APPENDICES

## ***APPENDIX 1*** CV

**EDUCATION**

*MSc Digital Forensics and Computer Security University Of Derby*

*Certificate Object Oriented Software Development Southern Alberta (OOSD) Institute Of Tech.*

*Certificate Information Security management Fanshawe College*

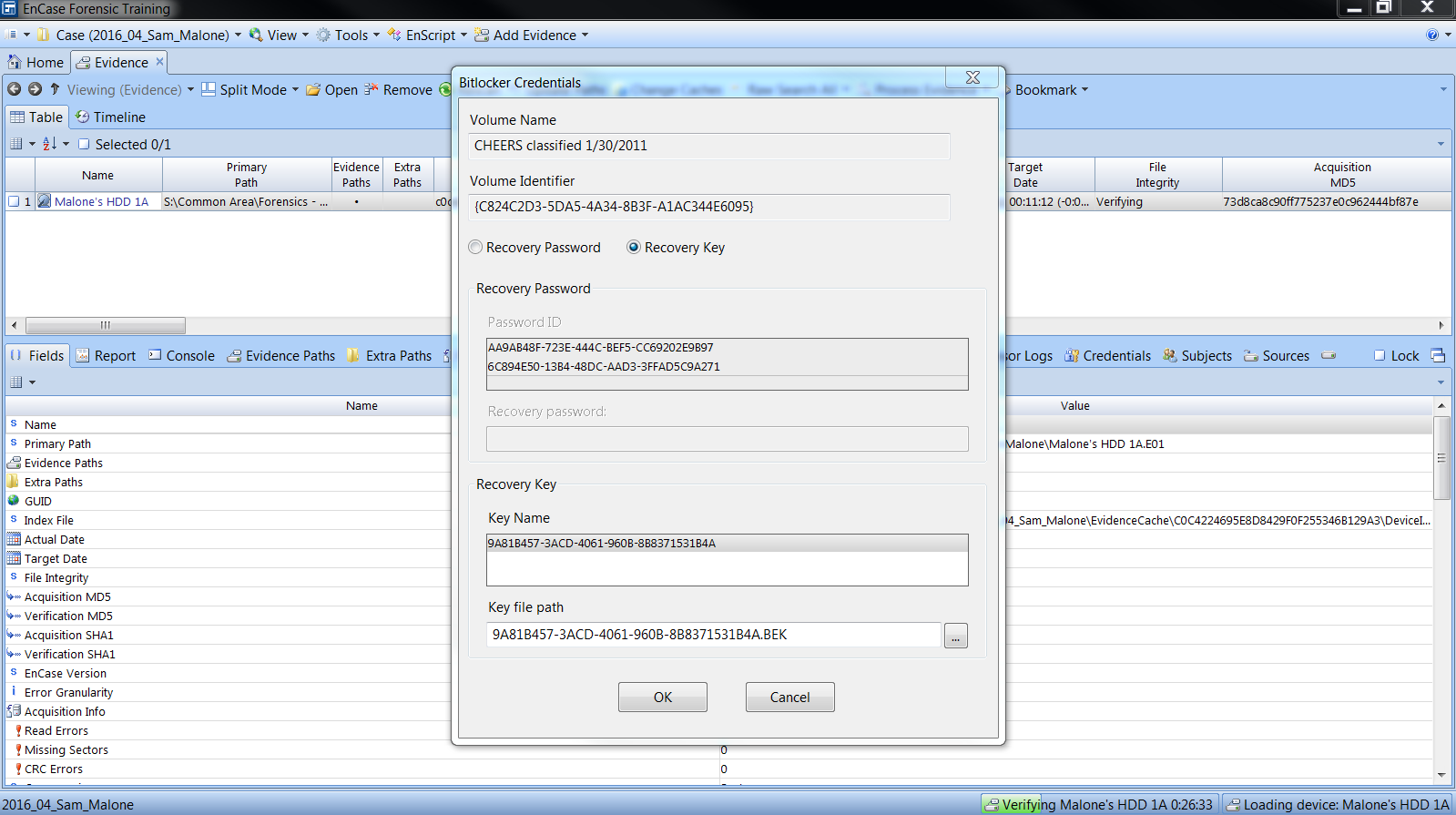
*Bachelor of Technology in Computer Science The Bells University*

***WORK EXPERIENCE***

*Database Analyst Casbade Group of Companies*

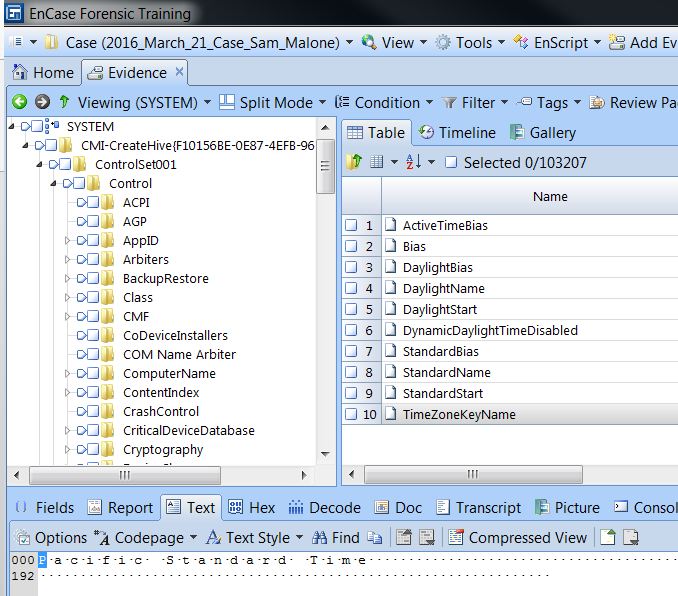
*IT Help Desk Fanshawe International Centre*

## ***APPENDIX 2 BITLOCKER***

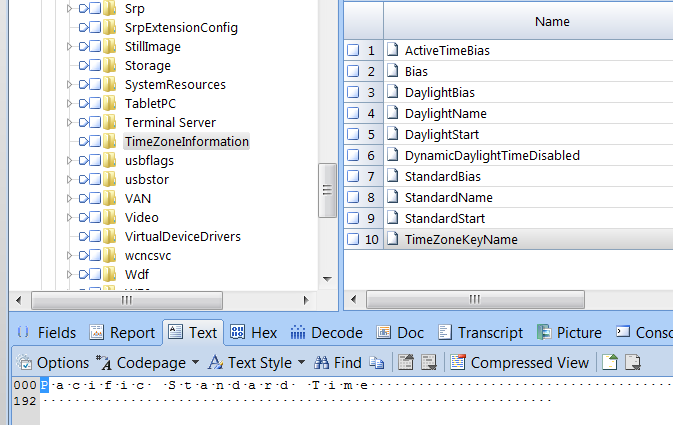


Appendix 2-i: Notification of the image being encrypted

## APPENDIX 3 TIME ZONE

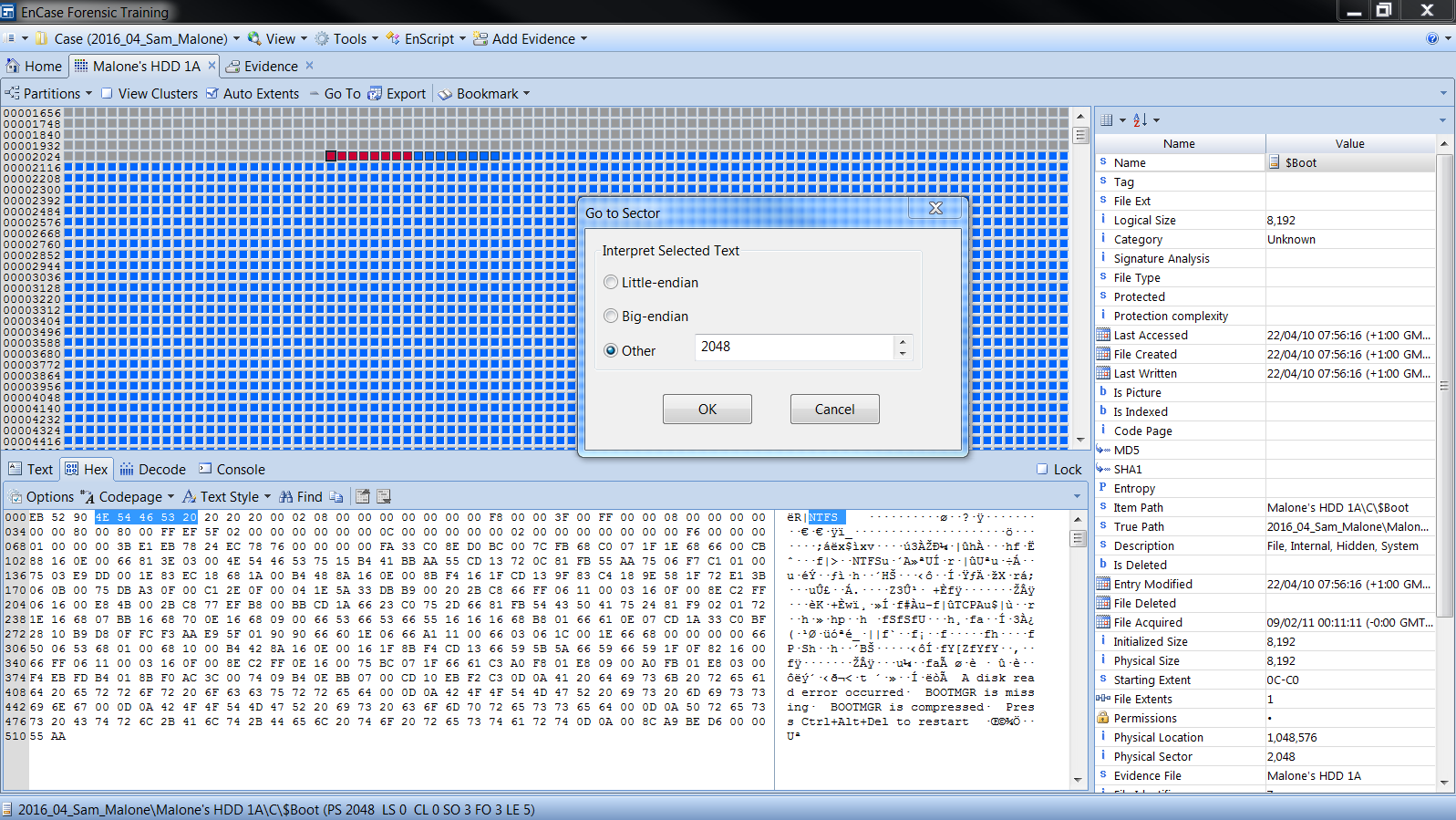


Appendix 3-I (Locating Time Zone)

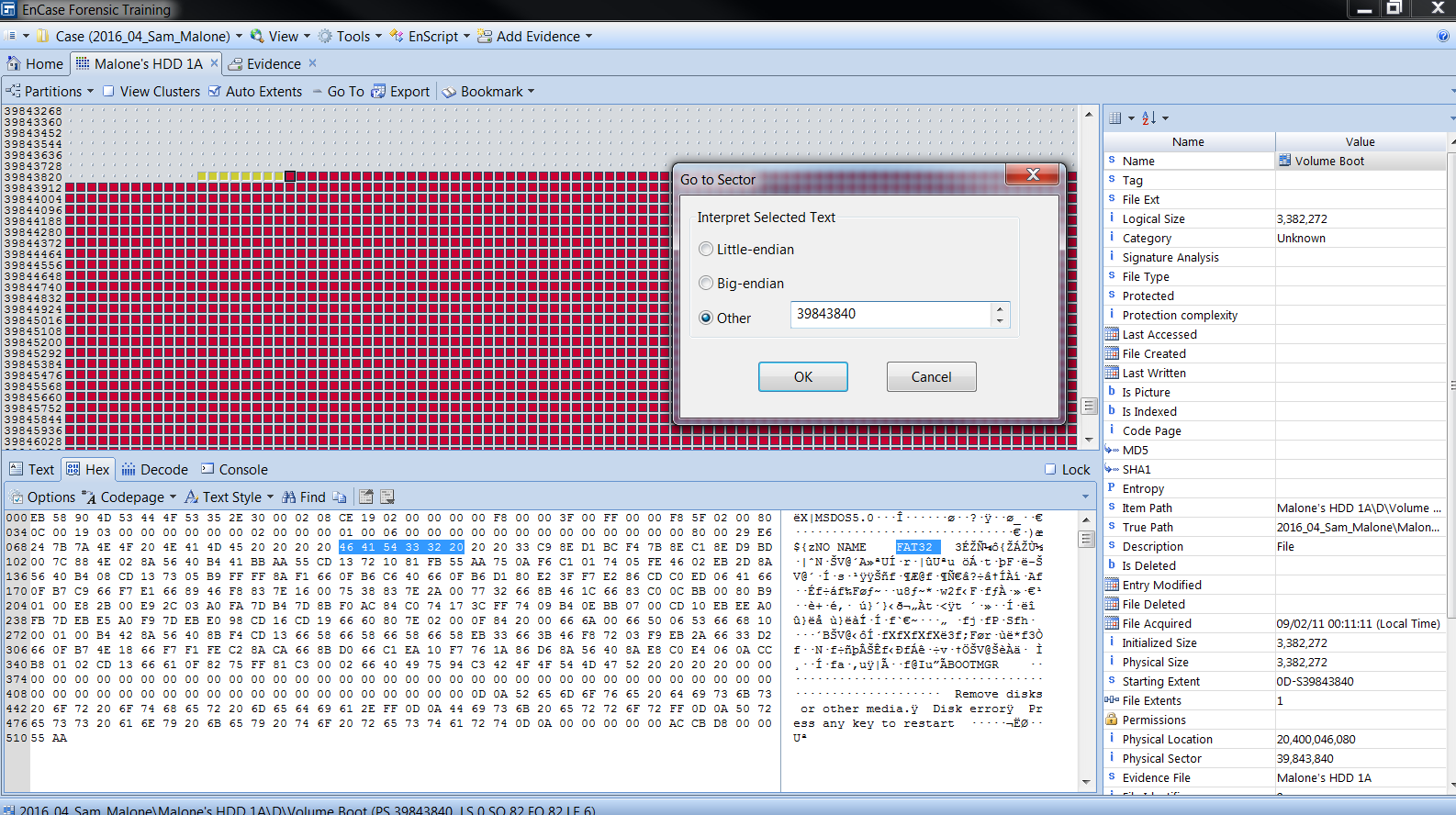


Appendix 3-ii (Locating Time Zone contd.)

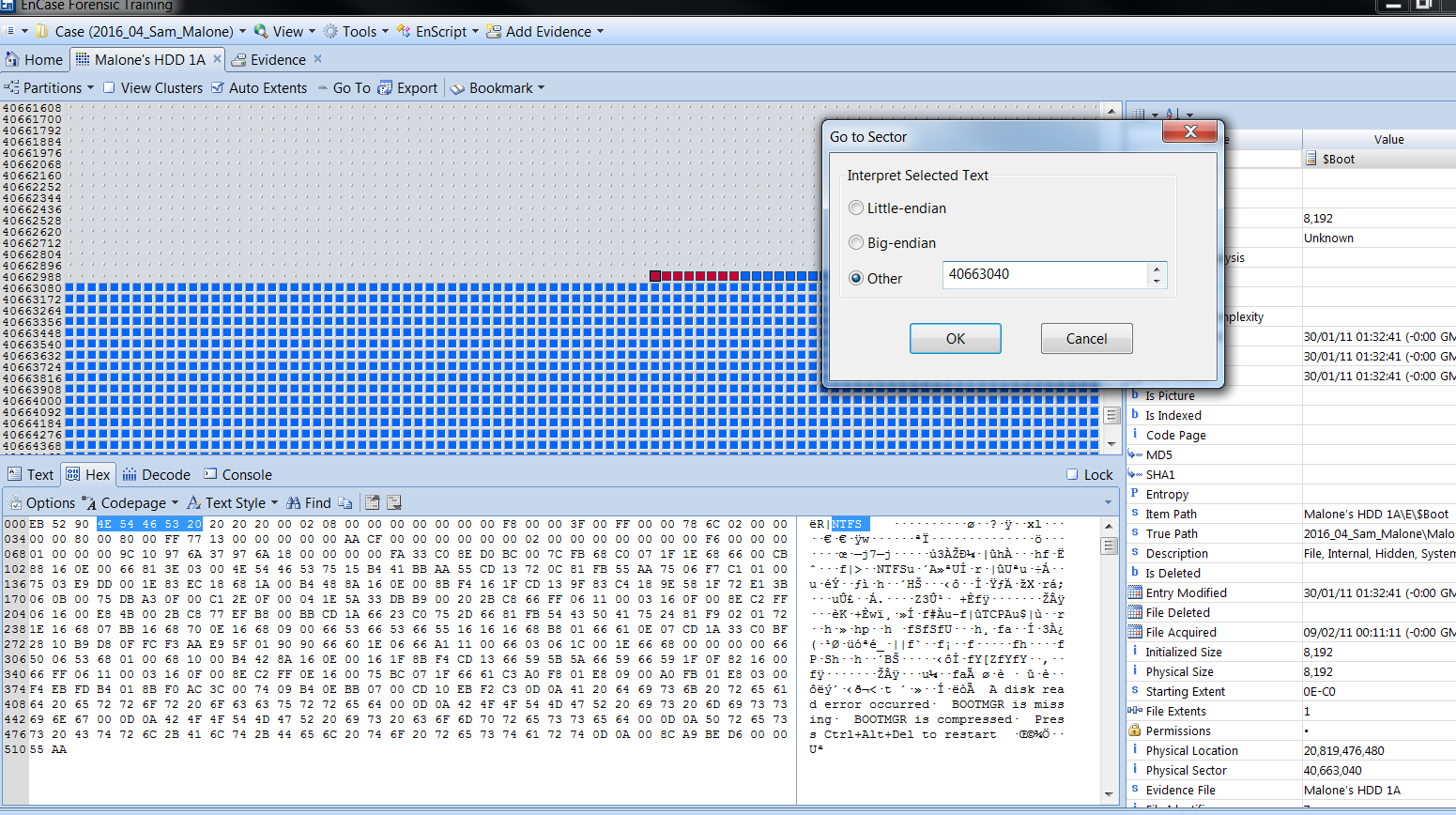
## APPENDIX 4 DISK ANALYSIS



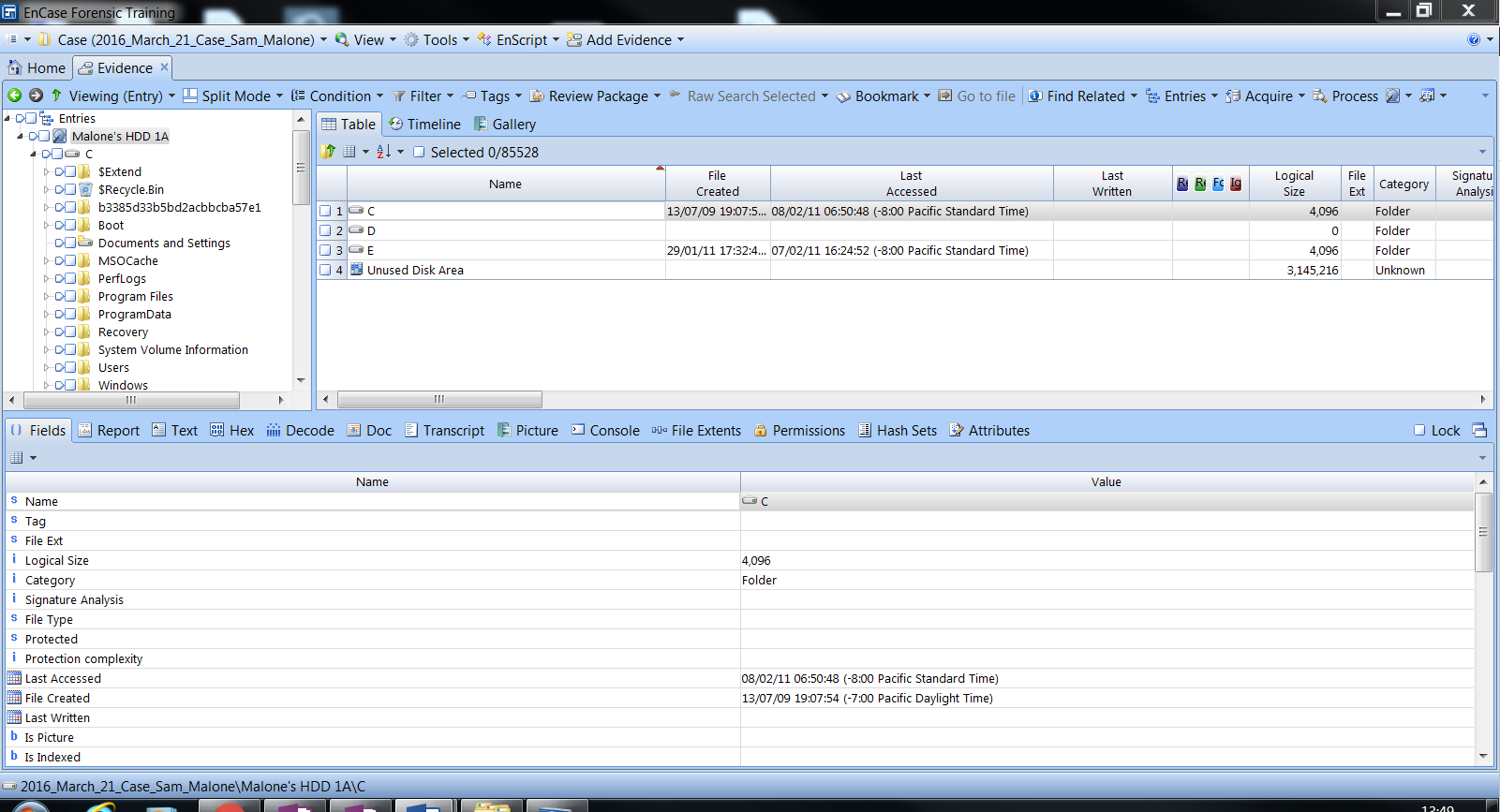
Appendix 4-i: NTFS Starting at Sector 2048



Appendix 4-ii: FAT32 Starting at Sector 39843840

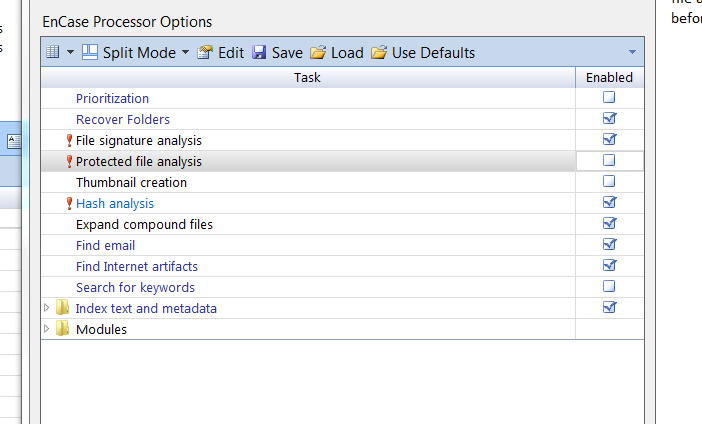


Appendix 4-iii: NTFS Starting at Sector 40663040



Appendix 4-ix: Retrieved Partition

## APPENDIX 5 EVIDENCE PROCESSING



Appendix 5-i: Evidence processing

## APPENDIX 6 EMAIL CONVERSATIONS & DOCUMENTS

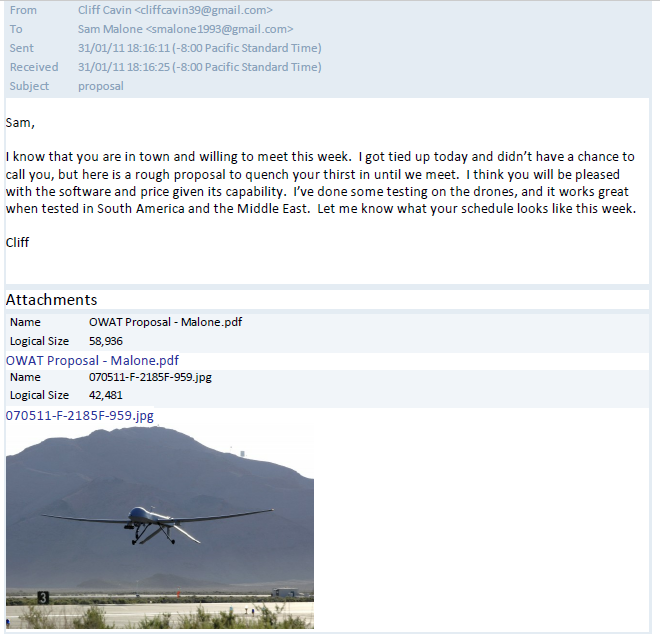
|  |  |  |  |
| --- | --- | --- | --- |
| ***Parties*** | ***Name*** | ***Email*** | ***Time Frame*** |
| *Defendant* | *Mr. Sam Malone* | [***smalone1993@gmail.com***](mailto:smalone1993@gmail.com) | *29/01/11 18:38:14 (PST)* |
| *Seller* | *Mr. Cliff Cavin* | [***cliffcavin39@gmail.com***](mailto:cliffcavin39@gmail.com) | *07/02/11 16:31:05 (PST)* |

|  |  |  |
| --- | --- | --- |
| ***Parties*** | ***Documents*** | ***Time Stamp*** |
| *Cliff contacting Sam* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\Inbox\query* | *29/01/11 18:40:42 (PST)* |
| *Cliff sends a proposal to Sam* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\Inbox\proposal* | *31/01/11 18:16:11 (PST)* |
| *Cliff sends Sam a presentation* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\Inbox\brief presentations\Cavin Weapons.ppt* | *02/02/11 16:59:03 (PST)* |
| *Cliff tells Sam to download TrueCrypt* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\Inbox\download TrueCrypt!* | *07/02/11 16:16:49 (PST)* |
| *Cliff sends Sam the Software* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\Inbox\the goods!* | *07/02/11 16:22:20 (PST)* |
| *Cliff’s Antigua Commercial Bank Account (89-2384993947) was funded with $22,950,000,000 by Mr. Malone* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\[Gmail]\Sent Mail\RE: the goods!* | *07/02/11 17:02:41 (PST)* |

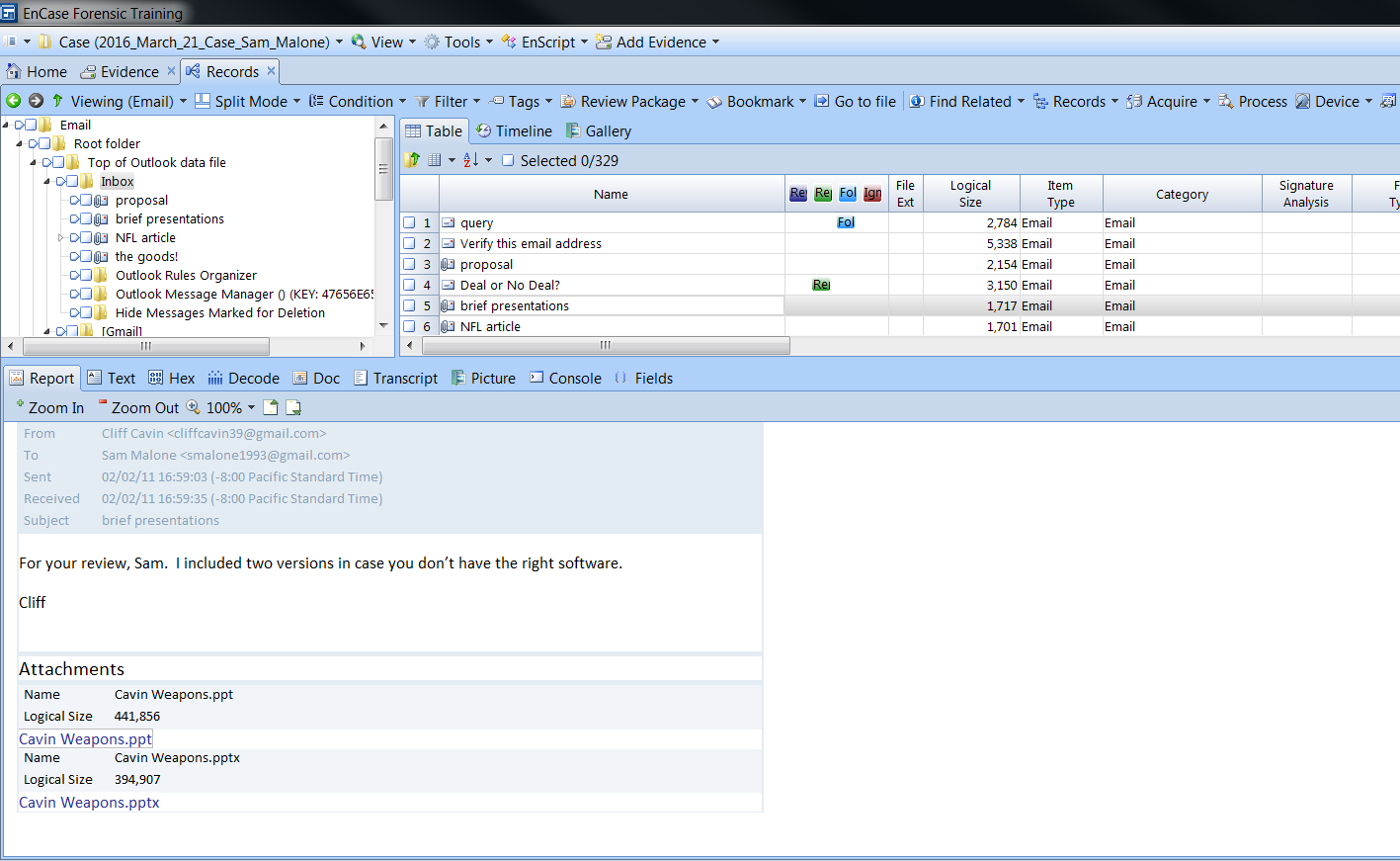
Appendix 6-i (email conversation)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Name*** | ***File Path*** | ***Time Stamp*** | | ***MD5*** |
| *Proposal: OWAT Proposal-Malone.pdf* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\[Gmail]\All Mail\proposal\OWAT Proposal - Malone.pdf* | *01/02/11 15:49:54 (PST)* | | *3f8a4dcb27f2271622b26fe83080a408* |
| *Drone: 070511-F-2185F-959.jpg* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\[Gmail]\All Mail\proposal\070511-F-2185F-959.jpg* | *01/02/11 15:49:54 (PST)* | | *ea5433430eff83ea7b189ee679e6267c* |
| *Final Cavin Weapons Purchase Order 2-7-2011.pdf* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\[Gmail]\All Mail\Deal! (Confidential)\Final Cavin Weapons Purchase Order 2-7-2011.pdf* | *07/02/11 15:58:30 (PST)* | | *2bcb41b479959ab555cf6f08f5b05046* |
| *Software: deal.jpg* | *C\Users\Sam.Malone\AppData\Local\Microsoft\Outlook\smalone1993@gmail.com.pst\Root folder\Top of Outlook data file\Inbox\the goods!* | *07/02/11 16:31:37 (PST)* | *f45cebf3db857fb173d289b9a7d63d02* | |

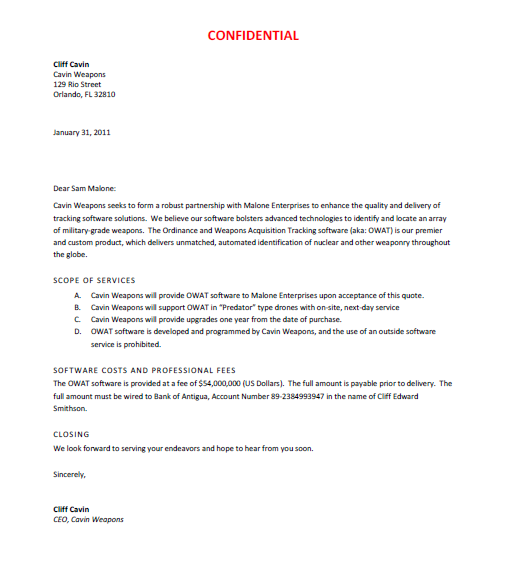
Appendix 6-ii (Documents)

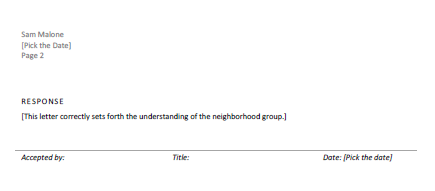


Appendix 6-iii

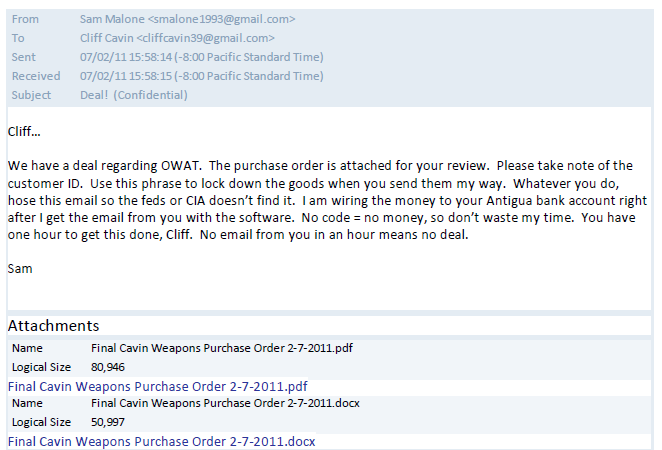


Appendix 6-iv

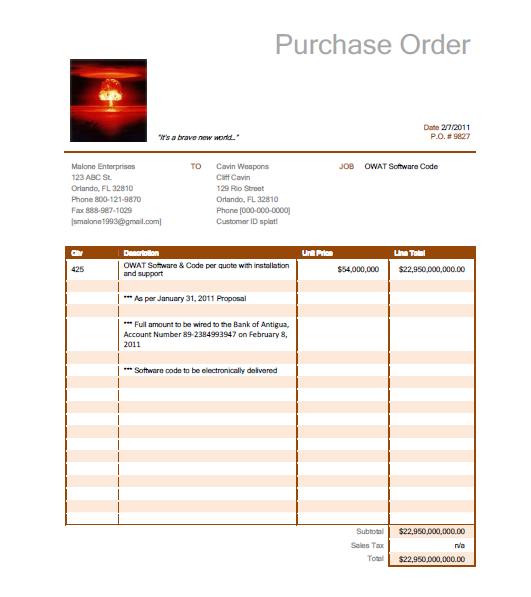




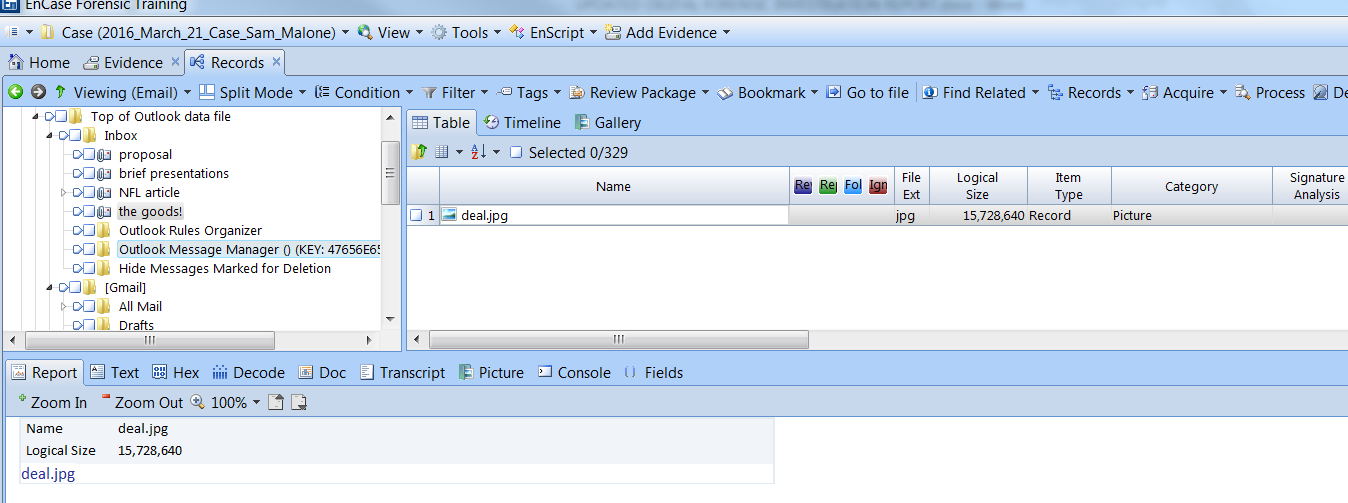
Appendix 6-v



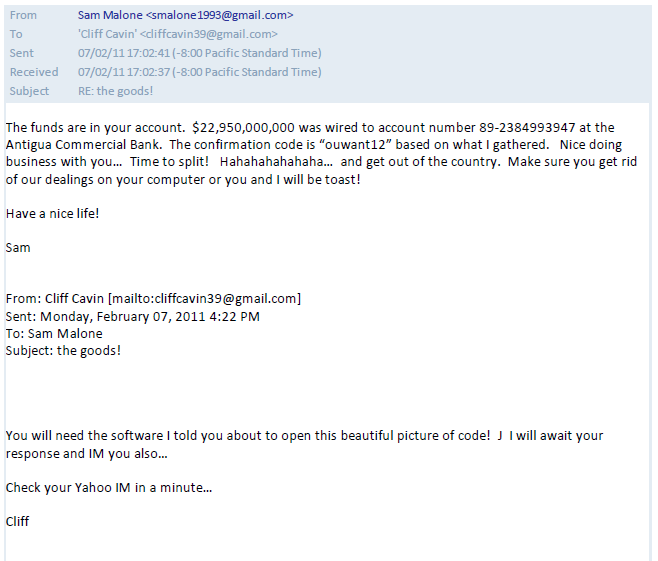
Appendix 6-vi



Appendix 6-vii Purchase Order

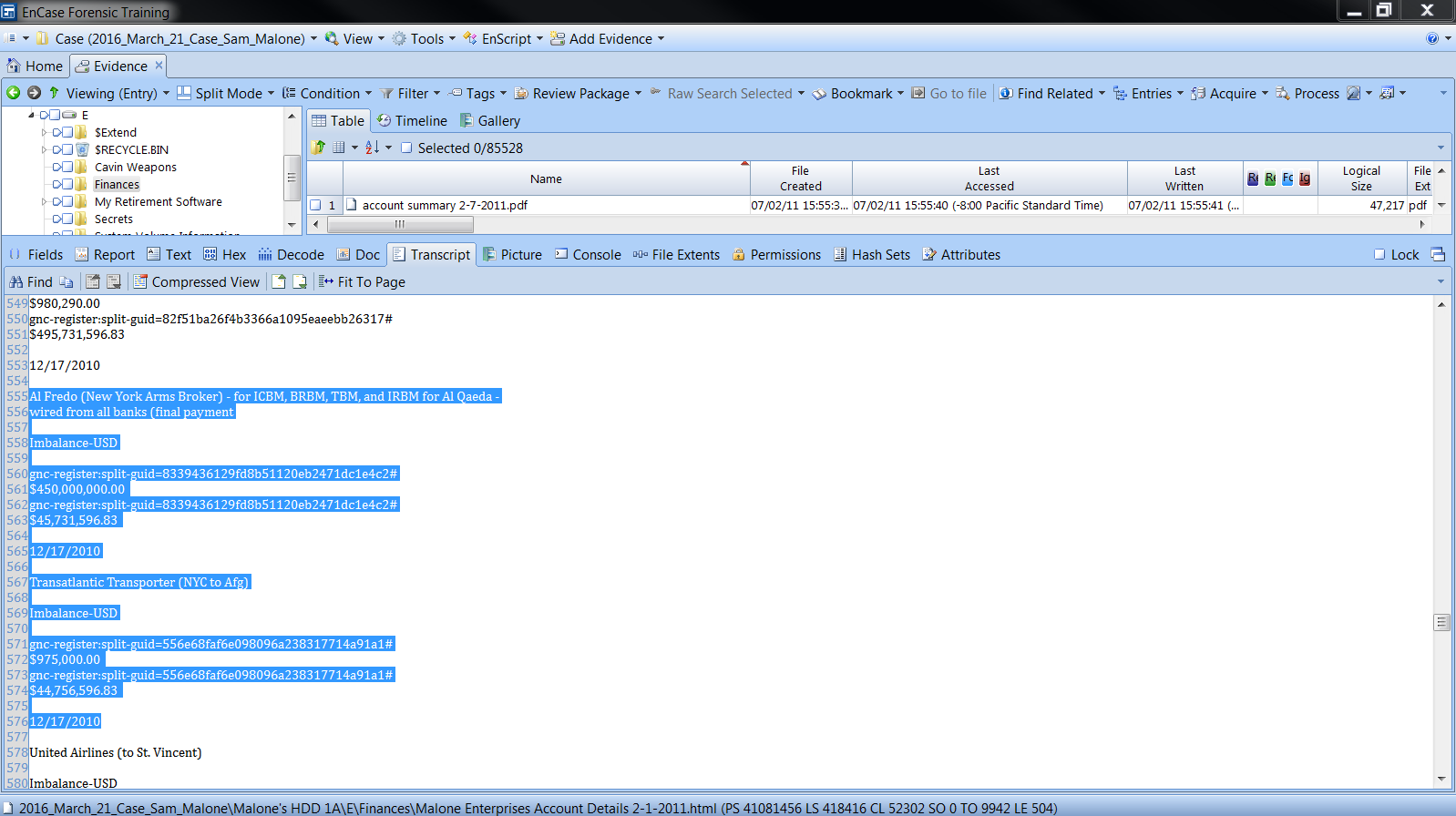


Appendix 6-viii The Software sent as a picture and encrypted (Steganography)

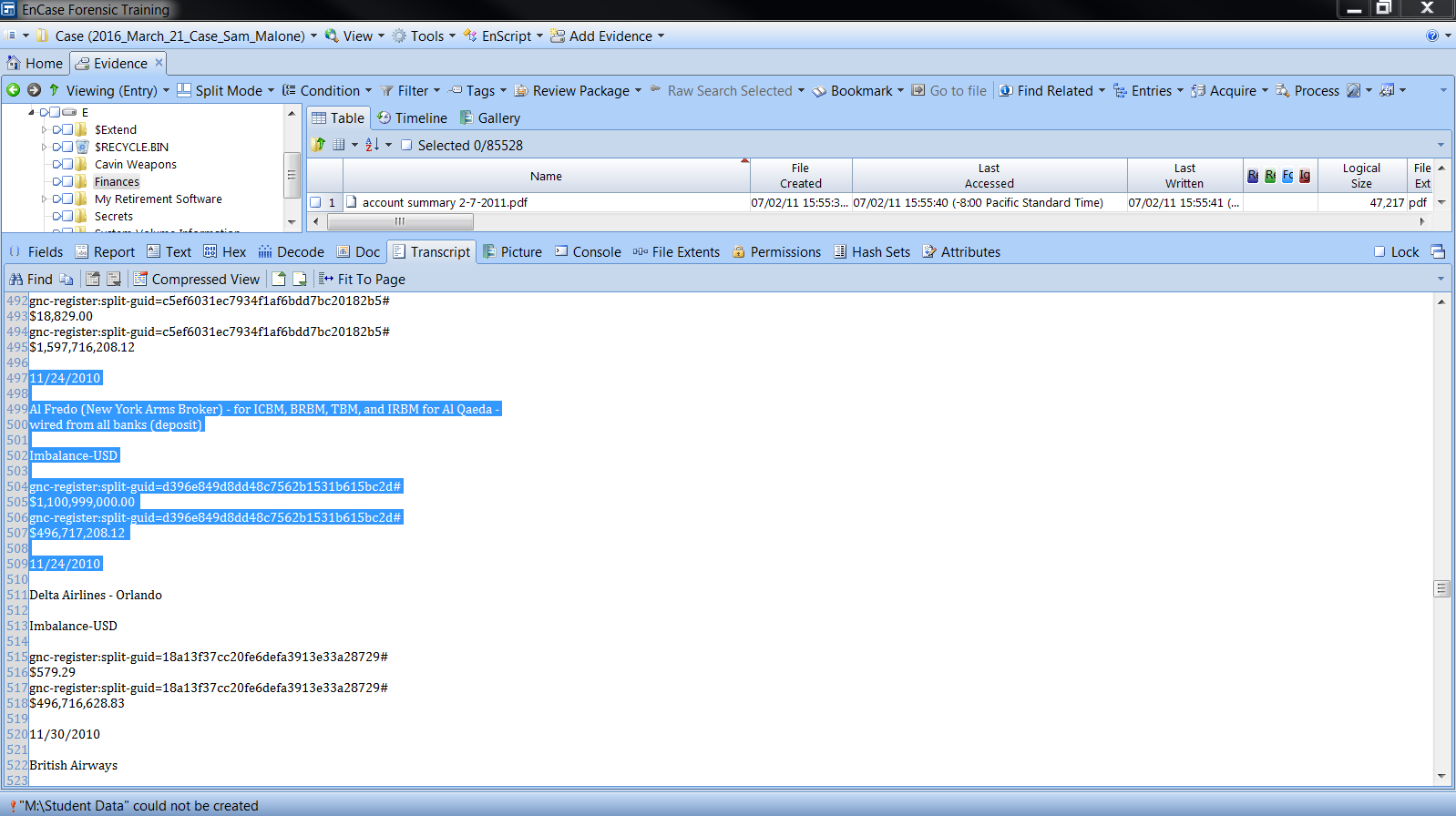


Appendix 6-ix Payment

## APPENDIX 7 ANALYSIS OF THE E DRIVE



Appendix- 7-i Received $450,000,000.00 from Al Qaeda through New York Arms Broker (Third Party)



Appendix- 7-ii Received $1,100,999,000.00 from Al Qaeda

|  |  |  |  |
| --- | --- | --- | --- |
| **Malone Enterprises Account Details 2-1-2011.html Containing Account Statement** | | | |
| ***PATH*** | ***Malone's HDD 1A\E\Finances\Malone Enterprises Account Details 2-1-2011.html*** | | |
| ***DATE*** | ***DESCRIPTION*** | ***TRANSACTION*** | ***BALANCE*** |
| *02/01/2010* | *Deposit - Dad's investment* | *$40,000.00* | *$40,000.00* |
| *02/10/2010* | *Deposit - DOD check* | *$2,857.00* | *$42,857.00* |
| *02/13/2010* | *1203 Garden Leasing (new office)* | *$5,287.00* | *$37,570.00* |
| *02/14/2010* | *Office Depot* | *$595.99* | *$36,974.01* |
| *02/15/2010* | *Dell Computers* | *$3,128.00* | *$33,846.01* |
| *02/26/2010* | *Al' Shiek-o-raza (investor)* | *$195,000.00* | *$228,846.01* |
| *02/26/2010* | *Blazin Customs (new car)* | *$56,983.00* | *$171,863.01* |
| *03/17/2010* | *United Airlines (Saudi-Egypt-Pakistan Trip)* | *$4,983.28* | *$166,879.73* |
| *03/17/2010* | *1204 Garden Leasing* | *$5,287.00* | *$161,592.73* |
| *03/19/2010* | *1205Deposit - DOD check* | *$6,948.83* | *$168,541.56* |
| *03/22/2010* | *Cash* | *$4,000.00* | *$164,541.56* |
| *04/02/2010* | *US Airlines (back to US)* | *$3,498.29* | *$161,043.27* |
| ***04/05/2010*** | ***Deposit - BoA MM*** | ***$775,000.00*** | ***$936,043.27*** |
| ***04/05/2010*** | ***deposit - Bank of Lativa*** | ***$4,289,000.00*** | ***$5,225,043.27*** |
| ***04/07/2010*** | ***deposit - Bank First Investments*** | ***$925,000.00*** | ***$6,150,043.27*** |
| ***04/09/2010*** | ***deposit - Citizens Bank of Costa Rica*** | ***$6,998,050.00*** | ***$13,148,093.27*** |
| ***04/27/2010*** | ***deposit - Prime Investments of Spain*** | ***$17,980,400.00*** | ***$31,128,493.27*** |
| ***04/29/2010*** | ***Crandum Technologies (wire)*** | ***$2,300,000.00*** | ***$28,828,493.27*** |
| *05/18/2010* | *Cash* | *$5,000.00* | *$28,823,493.27* |
| ***05/19/2010*** | ***Crandum Technologies (wire)*** | ***$2,700,000.00*** | ***$26,123,493.27*** |
| *05/19/2010* | *British Airways* | *$2,982.00* | *$26,120,511.27* |
| *06/08/2010* | *Ritz Carlton London* | *$15,928.00* | *$26,104,583.27* |
| *06/08/2010* | *Mears London* | *$2,090.87* | *$26,102,492.40* |
| ***06/24/2010*** | ***deposit - Prime Investments of Spain (cell 1)*** | ***$87,900,500.00*** | ***$114,002,992.40*** |
| ***06/24/2010*** | ***Al' Shiek-o-raza*** | ***$80,000,000.00*** | ***$194,002,992.40*** |
| ***07/08/2010*** | ***Alastair Engineering (hellfire)*** | ***$8,000,000.00*** | ***$186,002,992.40*** |
| ***07/08/2010*** | ***ArcLight Project (via Alastair)*** | ***$70,000,000.00*** | ***$116,002,992.40*** |
| ***07/22/2010*** | ***ArcLight Project (via Alastair)*** | ***$80,000,000.00*** | ***$36,002,992.40*** |
| ***08/19/2010*** | ***ArcLight Project (via Alastair)*** | ***$31,000,000.00*** | ***$5,002,992.40*** |
| *08/19/2010* | *Columbian Airlines* | *$4,987.29* | *$4,998,005.11* |
| *09/08/2010* | *Marriott* | *$11,087.99* | *$4,986,917.12* |
| *09/23/2010* | *Costa Rica Airlines* | *$1,409.00* | *$4,985,508.12* |
| *10/05/2010* | *British Airways* | *$2,311.00* | *$4,983,197.12* |
| *10/07/2010* | *Plaza Resort - Costa Rica* | *$17,984.00* | *$4,965,213.12* |
| *10/14/2010* | *Saudi Air* | *$1,905.00* | *$4,963,308.12* |
| *10/15/2010* | *Ritz Carlton London* | *$6,298.00* | *$4,957,010.12* |
| ***10/18/2010*** | ***Jumeirah (Dubai) Deposit for New Condo*** | ***$1,300,000.00*** | ***$3,657,010.12*** |
| *10/29/2010* | *Jumeirah (Dubai) Hotel* | *$14,992.00* | *$3,642,018.12* |
| ***10/29/2010*** | ***Al' Shiek-o-raza (Bank of Dubai)*** | ***$700,000,000.00*** | ***$703,642,018.12*** |
| ***11/01/2010*** | ***Adnan Gulshair el Shukrijumah (Bank of Dubai)*** | ***$900,000,000.00*** | ***$1,603,642,018.12*** |
| *11/01/2010* | *Virgin AIrlines* | *$5,952.00* | *$1,603,636,066.12* |
| ***11/04/2010*** | ***Estates of St. Vincent (deposit for home)*** | ***$5,900,000.00*** | ***$1,597,736,066.12*** |
| *11/10/2010* | *American Airlines* | *$1,029.00* | *$1,597,735,037.12* |
| *11/22/2010* | *Waldorf NYC* | *$18,829.00* | *$1,597,716,208.12* |
| ***11/24/2010*** | ***Al Fredo (New York Arms Broker) - for ICBM, BRBM, TBM, and IRBM for Al Qaeda -***  ***wired from all banks (deposit)*** | ***$1,100,999,000.00*** | ***$496,717,208.12*** |
| *11/24/2010* | *Delta Airlines - Orlando* | *$579.29* | *$496,716,628.83* |
| ***DATE*** | ***DESCRIPTION*** | ***TRANSACTION*** | ***BALANCE*** |
| *11/30/2010* | *British Airways* | *$2,837.00* | *$496,713,791.83* |
| *11/30/2010* | *Saudi Air* | *$1,905.00* | *$496,711,886.83* |
| *12/17/2010* | *Jumeirah (Dubai) New Condo Final Payment* | *$980,290.00* | *$495,731,596.83* |
| ***12/17/2010*** | ***Al Fredo (New York Arms Broker) - for ICBM, BRBM, TBM, and IRBM for Al Qaeda -***  ***wired from all banks (final payment*** | ***$450,000,000.00*** | ***$45,731,596.83*** |
| ***12/17/2010*** | ***Transatlantic Transporter (NYC to Afg)*** | ***$975,000.00*** | ***$44,756,596.83*** |
| *12/17/2010* | *United Airlines (to St. Vincent)* | *$6,829.00* | *$44,749,767.83* |
| *12/17/2010* | *Wire to Mom in FL* | *$20,000.00* | *$44,729,767.83* |
| *12/18/2010* | *Jumeirah (Dubai) Hotel* | *$19,807.00* | *$44,709,960.83* |
| ***12/21/2010*** | ***Estates of St. Vincent*** | ***$11,300,999.00*** | ***$33,408,961.83*** |
| *12/31/2010* | *St. Vincent Business Meeting and NY Party at Argyle* | *$79,000.00* | *$33,329,961.83* |
| *01/01/2011* | *United Airlines and carriers (to Pakistan)* | *$2,912.00* | *$33,327,049.83* |
| ***01/13/2011*** | ***Adnan Gulshair el Shukrijumah (Deposit for Weapons Software and Related***  ***Technologies)*** | ***$5,500,000,000.00*** | ***$5,533,327,049.83*** |
| *01/13/2011* | *United Airlines and carriers (to London)* | *$6,949.00* | *$5,533,320,100.83* |
| *01/14/2011* | *Marriott (Islamabad)* | *$3,029.00* | *$5,533,317,071.83* |
| *01/20/2011* | *British Airways to Orlando* | *$1,970.80* | *$5,533,315,101.03* |
| ***01/22/2011*** | ***Al Fredo (New York Arms Broker) - for ICBM, BRBM, TBM, and IRBM for Al Qaeda*** | ***$2,277,400,900.00*** | ***$3,255,895,291.03*** |
| ***01/24/2011*** | ***Sunset Tech (Predator - $4.5 Million X 100)*** | ***$450,000,000.00*** | ***$2,805,895,291.03*** |
| ***01/24/2011*** | ***Transatlantic Transporter Plane (NYC to Pakistan)*** | ***$5,600,000.00*** | ***$2,800,295,291.03*** |
| *01/24/2011* | *wire to Aunt in DC* | *$10,000.00* | *$2,800,285,291.03* |
| ***01/25/2011*** | ***Transatlantic Transporter Plane (FL to Pakistan)*** | ***$22,000,000.00*** | ***$2,778,285,291.03*** |
|  |  |  |  |

*Table 7: Malone’s Account Statement*

* *Transactions above $500,000.00 are bolded*
* *Transactions of high risk are bolded and in red*

## APPENDIX 8 GLOSSARY

***Image file****: Forensically sound and a total duplicate of a digital media tot eh last bit, which can be used as an evidence.*

***Verification:*** *A testing process to find out if a thing or an event is accurate, positive or true*

***Path:*** *The place in which something is stored*

***BitLocker:*** *A feature that is designed to secure data by providing full encryption for disks*

***hash:*** *A fixed length of strings used for verifying the integrity for a file*

***Identification:*** *This is the finding of potential source of digital evidence* (Casey, 2004)

***Preservation:*** *This is the securing and maintenance of documents and evidences associated with the investigation* (Casey, 2004)