2012 Third International Conference on Emerging Intelligent Data and Web Technologies

Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institutions

Denys A. Flores [*#1], Olga Angelopoulou [*2], Richard J. Self [*3]
[*]University of Derby, Faculty of Business Computing and Law, Kedleston Road, Derby, DE22 1GB, United Kingdom
[#]National Polytechnic School, Department of Informatics and Computer Sciences (DICC), Quito, Ecuador
[1]d.flores1@unimail.derby.ac.uk; denys.flores@epn.edu.ec
[2]o.angelopoulou@derby.ac.uk
[3]r.j.self@derby.ac.uk

***Abstract*— Digital forensics is the science that identify, preserve, collect, validate, analyse, interpret, and report digital evidence that may be relevant in court to solve criminal investigations [1] [2]. Conversely, money laundering is a form of crime that is compromising the internal policies in financial institutions, which is investigated by analysing large amount of transactional financial data. However, the majority of financial institutions have adopted ineffective detection procedures and extensive reporting tasks to detect money laundering [3] without incorporating digital forensic practices to handle evidence. Thus, in this article, we propose an *anti-money laundering model* by combining digital forensics practices along with database tools and database analysis methodologies. As consequence, admissible Suspicious Activity Reports (SARs) can be generated, based on evidence obtained from forensically analysing database financial logs in compliance with *Know-Your-Customer policies* for money laundering detection [4].**

Keywords-digital forensics; database log; business intelligence; BI; MySQL; store procedure; extractor; ETL; SAP; FTK

I. Introduction

Digital forensics is part of the forensic science [1] which aims to identify, preserve, collect, validate, analyse, interpret, document and present digital evidence stored in electronic sources; e.g. a computer. As a result, these practices can be used to either facilitate the reconstruction of events during criminal investigations, or anticipate unauthorised actions [2]. Furthermore, these techniques can be used not only for criminal, but also for civil litigations [5] including money laundering, which is a form of financial fraud that has been evolving since 2001 due to the advantages of technology [2].

Conversely, considering that digital forensic tools might not be appropriate to analyse large amounts of transactional data stored in database servers [6], the application of internal controls has been suggested to track illegal financial transactions [7]. Particularly, the most important *anti-money laundering internal controls* are the *Know-Your-Customer 'KYC' policies* since they define the guidelines for detecting *illegal customer transactions* in order to generate reliable *Suspicious Activity Reports 'SARs'* [8].

Nonetheless, the current research has found that majority of these internal controls, including *KYC policies,* are outlined within *anti-money laundering procedures* which are intensive to create and maintain, making them ineffective and most likely to be deviated by money launderers [3]. Moreover, when these controls are closely related to database logs, both enterprise applications and database tools cannot reduce the data volume to analyze in order to undertake a successful forensic investigation [9]. Similarly, due to both the limited audit capabilities in database management systems (DBMS), and some flaws in database configuration [6], the efforts to preserve historical database records, in order to enhance the detection of suspicious activities may be affected [10].

Finally, even though the *Financial Action Task Force*[1] *'FATF'* issued a set of best practices in order to detect money laundering [8] [4] [11], it has been found that they do not provide a process, or a well-defined strategy to achieve this aim. Also, the complexity of this form of crime restricts the definition of a standardised approach to track illegal financial proceedings, the sources of which may be not only financial fraud, but also predicate offences such as terrorism financing, human trafficking, drug dealing, among others [4].

Therefore, we propose an *anti-money laundering model* which combines digital forensic practices as well as database tools and database analysis methodologies in order to align them with the *KYC policies.* Hereby, the detection of this form of crime can be enhanced by analysing customers' financial transactions, regardless the subjacent offences. Consequently, relevant *SARs* can be delivered by conducting the following activities in order to obtain admissible financial evidence:

(1) Retrieve relevant information from large financial databases using *store procedures,* in order to *generate database logs* of suspicious transactions based on the thresholds defined in the *KYC policies*

(2) Consider these *database logs as evidence*, and analyse them using *digital forensic approaches and tools*, so they can be used as admissible evidence in court, and

(3) Use *database analysis methodologies,* like Business Intelligence (BI), to enhance the presentation of suspicious activity reports (SARs) [8].

Hence, in section II, the importance of digital forensics as an anti-money laundering strategy is explained. In section III, some challenges for adopting digital forensic practices and anti-money laundering detection strategies

[1] The *FATF* is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing [31].

978-0-7695-4734-3/12 $26.00 © 2012 IEEE
DOI 10.1109/EIDWT.2012.22

inside organisations are discussed. Then, in section IV, a model to detect money laundering activities is proposed by combining digital forensics practices and database analysis. Also, in order to illustrate the application of the model, an example of money laundering detection is explained, using *MySQL Server*, as target system, and *SAP Crystal Dashboard Designer as BI analysis tool* to present the results during a money laundering case. Finally, conclusions about this research are given.

II. Importance of Digital Forensics as an Anti-Money Laundering Strategy

Digital forensic practices are currently an established field in criminal and civil investigations, which have been extended inside the enterprises to associate digital investigations with incident response [12]. As a result, illegal activities carried out by employees can be tracked to assure legal compliance and a fresh record of audit trails [13]. However, these illegal activities are not only done by employees, but also by customers. A case in point is money laundering which is a criminal activity to change illegal income into legal [3], using financial institutions as means of this crime. Hence, due to the fact that money laundering activities have to be investigated inside the financial institution in order to provide the *Financial Intelligence Unit*[2] with admissible evidence for conducting further legal actions [11], the adoption of forensic computing practices is mandatory and important in order to:

- Support the detection of money laundering
- Facilitate the 'e-discovery' process in civil litigations linked to money laundering by using databases as a forensic tool
- Assess the effectiveness of IT governance, compliance, and security

First, financial institutions should adopt digital forensic practices in order to detect money laundering by investigating fraudulent transactions [14]. In fact, money laundering is currently linked not only to drugs and terrorism [8], but also to cyber fraud [3]. Moreover, the lack of practices to forensically investigate illegal activities inside financial institutions may cause that digital evidence linked to money laundering is dismissed in court [15]. Nonetheless, even though digital evidence is difficult to identify and collect due to the intangible value of data, many records, and audit trails can be obtained using digital forensic support [12].

Second, considering that 'e-discovery' involves finding admissible digital evidence or 'electrically stored information' (ESI) linked to civil cases, it is the duty of an investigator to provide relevant ESI by means of digital forensic techniques [16]. For instance, if the crime is related to money laundering, database tools can be used to extract and analyze relevant evidence for anti-money laundering purposes. As consequence, forensic techniques and database analysis can help to quickly deliver concise suspicious activity reports (SARs) with high understandability in electronic form, instead of using paper copies [17].

Finally, applying money laundering procedures based on digital forensic practices inside the financial institutions can help the organisation to assess the effectiveness of controls and procedures related to information security compliance [14]. Meanwhile, in the context of money laundering, digital forensic procedures allows analysing suspicious transactions to support internal audits and risk compliance evaluations. Consequently, more concise reports can be delivered by linking digital evidence with specific persons to prove that someone did or did not commit the crime [5].

Summing up, we propose to adopt digital forensic practices inside financial institutions in order to support the detection of money laundering by forensically analysing database records to generate admissible evidence. Also, by using database tools, the extraction and analysis of relevant financial evidence can be enhanced. Subsequently, the production of SARs can be supported by clear timeline descriptions based on admissible digital evidence during e-discovery cases related to money laundering. At last, the adoption of digital forensic strategies can help the organisation to achieve strategic goals for money laundering detection, supported by tools and IT procedures which can align the IT strategies with the anti-money laundering objectives.

III. Challenges of Anti-Money Laundering Detection Strategies and Digital Forensic Practices within Organisations

The adoption of anti-money laundering strategies inside financial institutions has some challenges, so does the implementation of digital forensic practices to enhance the detection of this kind of crime. In the following sub sections, some general challenges related to anti-money laundering detection are discussed.

A. Ineffective Money Laundering Procedures

Anti-money laundering procedures in financial institutions are intensive to create, and maintain even though they are supported by automated tools to detect suspicious activities [3]. Moreover, extensive research [17] [18] has found that although these rule-based procedures follow international best practices and recommendations, they have an inherent low efficiency due to the fact that criminals may obtain unauthorized access to them in order to learn, and evade their rules. In fact, the problem is not just an organisational fault, but a general issue derived from the evolution of technology which causes the lack of both the standardization of existent digital forensic procedures, and the constant training of digital forensic investigators [19].

In contrast, according to 'principle 3' of the ACPO guidelines [20], a third party should be able to replicate the steps to collect digital evidence producing the same result. However, since digital evidence can be collected by using

[2] Also Known as *FIU,* is a financial intelligence organisation which analyzes information that has been reported via SARs, concerning unusual or unjustified financial operations or transactions [28]

flawed procedures through experiments in controlled environments [15], the approach followed in the investigation may be questionable, and the evidence may be discarded.

At last, although this research has not found any money laundering detection procedures based on digital forensic practices, adopting them inside the organisations is important not only for defining adequate incident management strategies [2], but also for responsibly handling digital forensic evidence related to money laundering events.

B. *Underestimation of Digital Forensic Practices inside the Organisations*

Organisations underestimate the collection of digital evidence [14]; specifically, when it is required to prove fraudulent transactions in order to link the attacker with the incident. In addition, this may be the result of an over reliance in 'SARs', the reporting tasks of which are very slow due to the time required in the collection of large volumes of data [17]. In fact, even though powerful data analysis tools can be used in producing these reports, the time required to analyze the evidence cannot be easily reduced [9]. Furthermore, organisations omit the fact that not all the evidence is relevant at the end, so thinking about adopting digital forensic practices may seem operatively costly [14].

Therefore, digital evidence acquisition to support money laundering detection must not rely on large and time-consuming reporting tasks, but in the support provided by data analysis of suspicious transactions using digital forensic approaches.

C. *Lack of Training in Digital Forensic Practices*

Another problem for financial institutions may be the lack of trained personnel in digital forensic practices, which is a clear disadvantage [1] [9]. Moreover, the lack of proactive digital forensic practices inside the organisations are costly considering the number of man-hours in incident response strategies, disaster recovery plans, and business continuity goals [14]. Also, inside financial institutions, the lack of training and analysis capability of employees is even worse when there are few people with scarce technical support for decision making [17]. Furthermore, in order to analyze the information stored in databases, it is necessary to understand how the data is being built [21] so that a consistent report can be delivered. However, fraud auditors in financial institutions do not know the data structures used in transactional databases [22], which definitely represents a disadvantage in money laundering detection.

Conversely, the misunderstanding of digital forensic practices is a problem since digital investigations inside financial institutions may involve servers containing large amount of information [12]. Hence, untrained personnel in charge of money laundering detection may not follow digital forensic techniques, which may lead to overestimate evidence; e.g., determining whether a money laundering event is just linked to a few transactional records in comparison to the entire transactional logs [5].

As a result, this implies not only a waste of time and resources to investigate an isolated event, but also may cause that the evidence is dismissed in court.

D. *Privacy Issues*

Complex digital forensic cases may generate large data volume [9]; specifically, due to anti-money laundering policies which urge financial institutions to keep records of their customers for at least 5 years [17]. In contrast, analysing and processing large volume of private information during digital investigations [6] can raise problems regarding the customers' privacy rights due to the risk of unwanted disclosure of personal information [10].

Thus, a digital-forensics-based detection model is proposed and explained in the next section in order to outline a straightforward process to include in any detection procedure for its reinforcement. Also, since the model proposes aligning digital forensic practices with the *Know-Your-Customer policies,* financial institutions can be aware of the importance of adopting digital forensics to enhance analysis and reporting tasks during money laundering investigations. Moreover, by adopting this model, it is expected that financial institutions are more resilient to train their personnel in forensic computing practices, and therefore, manage money laundering evidence, including customer information, in a forensically sound manner to avoid privacy breaches.

IV. ANTI-MONEY LAUNDERING DETECTION MODEL BASED ON DIGITAL FORENSIC PRACTICES AND DATABASE ANALYSIS

Digital forensic practices do not consider the aspects of IT governance related to transactional databases [14]. Moreover, traditional digital forensic practices may not be suitable to analyze large amount of data stored in database servers [23]. Hence, combining digital forensic practices and tools with database analysis is important to enhance the effectiveness of anti-money laundering detection inside financial institutions.

First, digital forensics practices *per se* do not cover the proactive application of tools to improve the IT governance inside organisations [14], because these practices are mainly focused on evidence identification, collection, handling, storage, incident response and training [9]. Moreover, even though money laundering activities may be difficult to trace, they can be detected when all the important information within the database is monitored [6]; thus, digital investigations have to be complemented with database analysis in order to conduct successful anti-money laundering investigations.

Then, traditional digital investigations require shutting the target system down, and the physical removal of the hard drive for its later imaging [12]. However, if the target system is a database server, removing and imaging its hard drive is counterproductive because production servers are huge data storages which cannot be shut down, and their drives may be far larger than any external drive in the market, so they may not be possible to image into a standard external drive [23]. Thus, imaging just the relevant evidence, like important transactional logs related to suspicious transactions, should be considered. In order to do this, the 'database log environment' has to be controlled for producing specific logs to record suspicious transactions, using simple SQL procedures to support the investigation.

Hence, an anti-money laundering model (Fig. 1) is explained to handle digital evidence, considering the stages suggested by Grobler, et al. [14] 'before, during, and after an incident' takes place along with the 'Case-Oriented Evidence Model' proposed by Zhang and Wang [9] in order to understand, analyze, evaluate, and report a case.

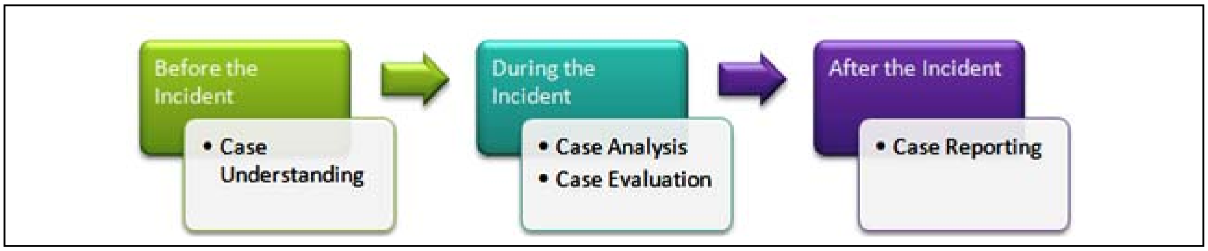


Figure 1. Anti-Money Laundering Model combining the stages suggested Grobler, et al. [14] and the Case-Oriented Evidence Model [9]

A. Before the Incident: Case Understanding

Before an incident takes place, it is recommended to understand the case [9]. First, in case of money laundering, the *Know-Your-Customer 'KYC' policies* in the financial institution should be analysed. In fact, understanding these policies can support the detection process by defining thresholds according to the organisational goals [22] to prevent money laundering.

As consequence, they can be analyzed using databases to prove that the defined *KYC policies* have been violated [24]. For instance, if an indicator 'greater than or equal to a specific amount of money' has been defined, transactions may be considered suspicious when they match these criteria within a period of time.

Similarly, since valuable evidence may be available within databases [6], identifying the possible sources of information like accounting databases is necessary. Also, non-accounting databases, like customer information, have to be identified along with non-electronic data sources which must be transferred to electronic formats [22].

B. During the Incident

Case Analysis: During the incident it is necessary to observe the case conditions, and determine how and where the evidence should be obtained. Once the relevant data sources have been identified, the top-down approach [9] can be used to identify and store the relevant fields in one single *de-normalized database table*[3]. Then, considering the importance of preserving events in a common database table for further forensic analysis [25], the examination sequence to acquire and examine the relevant data fields has to be done as follows:

a) Data Acquisition (Fig. 2):

- Identify the data sources to support the thresholds defined by the *KYC policies* in the organisation, and create a de-normalised table to store relevant information extracted from the data sources already identified [22]. To illustrate this, a de-normalised table was created using *MySQL Server,* which was populated with 100 fictitious records to emulate banking transactions whose fields may be: *Name, Surname, Company Name, Customer Id, Address, Telephone, Transaction Type (Credit/Debit/Transfer), Transaction Nº, Amount and Date*

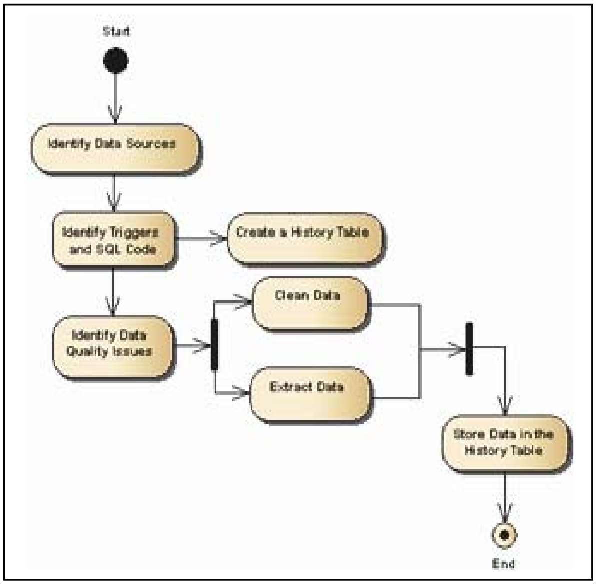

Start
Identify Data Sources
Identify Triggers and SQL Code
Create a History Table
Identify Data Quality Issues
Clean Data
Extract Data
Store Data in the History Table
End

Figure 2. Data Acquisition activities

- Identify useful triggers and SQL code that may be already present in the database in order to re-use them to provide additional levels of logging and recording [23].
- Identify data quality issues that can affect the evidence due to incomplete and inaccurate data as well as inappropriate data granularity and wrong formats [22].
- Clean the data before extraction by following the *Extraction, Transformation and Load (ETL) practices*

[3] D*e-normalization* is the process to optimise the read performance of a database by adding or grouping redundant data [29].

for Data Warehousing[4]. Thus, as digital evidence storages can be different computers or different data sources [12], only the relevant data securely tested, and cleaned is stored in the de-normalised table.

- Creating store procedures [24] as extractors allows creating log files from the 'de-normalised table' using database queries. For example, this store procedure in MySQL Server:

```
delimiter $$
    USE `sample_database`$$
    CREATE PROCEDURE
    `backup_transactions_csv` (IN amount
    DECIMAL, IN start_date DATETIME, IN
    end_date DATETIME)
    BEGIN
     SET @threshold = amount;
     SELECT * FROM
     `sample_database`.`tb_db_transact_log`
         WHERE
         `tb_db_transact_log`.`trans_amnt`
         >= @threshold AND trans_datetime
         BETWEEN start_date AND end_date
    INTO OUTFILE '/home/root/Documents/MySql
         Forensic Logs/backup.csv'
         FIELDS TERMINATED BY ','
         OPTIONALLY ENCLOSED BY '"'
         LINES TERMINATED BY '\n';
    END
$$
```

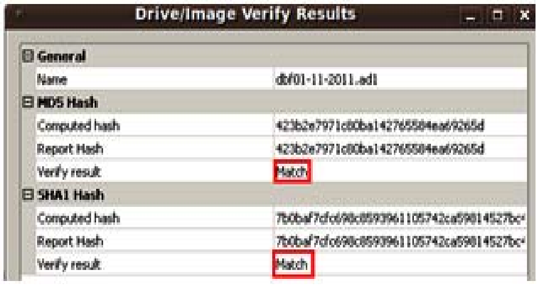
Then, using the previous store procedure code, database logs can be created, and stored as plain text; e.g., creating CSV files as suspicious database logs from Jan. to Mar. 2011 when transactions are greater or equal than USD$ 10,000. 00:

```
-- Backup Jan11 - Mar11
DELIMITER $$
USE `forensics`$$
CALL backup_transactions_csv(10000.00,
'2011-01-01', '2011-03-01');
```

Although, the whole database should be examined to detect frauds [22], if the proper data sources have been identified, there is no need to examine the whole database, because the extractors can filter the information automatically and store it in customized database logs, ensuring the normal server's function by planning and targeting the database activities [23]. Also, in case that more evidence needs to be obtained, the extractors can be executed as many times as needed to create new logs for further analysis.

b) Data Examination:

Database log files can be digital evidence. However, these have to be extracted by *selectively imaging* [12] just the folder where they are stored in the server, according to 'principle 1' of the *ACPO guidelines* to avoid evidence corruption and manipulation [20]. For example, *FTK Imager* has been used to create an image of the database log folder (Fig. 3).

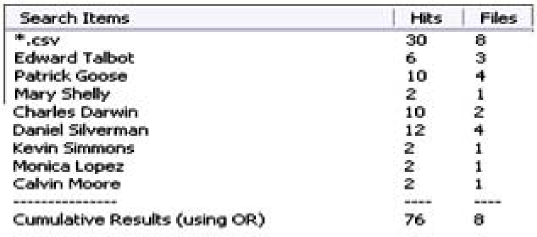


⊟ General	
Name	dbf01-11-2011.ad1
⊟ MD5 Hash	
Computed hash	423b2e7971c80ba142765584ea69265d
Report Hash	423b2e7971c80ba142765584ea69265d
Verify result	Match
⊟ SHA1 Hash	
Computed hash	7b0baf7dfc698c8593961105742ca59814527bc
Report Hash	7b0baf7dfc698c8593961105742ca59814527bc
Verify result	Match

Figure 3. Database log folder imaging using FTK Imager

2) Case Evaluation: After examining the evidence, it is necessary to review the findings to ensure that all important aspects have been considered. In fact, by adapting the 'top-down' approach suggested by Zhang and Wang [9] into money laundering detection, the extracted database logs can be analyzed to find specific information related to possible money launderers. This must be performed following these stages:

a) Data Analysis: Current enterprise tools do not provide audit controls to monitor the access/owners of specific data [12]. Therefore, the evidence can be validated [7] using a digital forensic analysis tool like *FTK* (Fig. 4) so that the imaged log directory can be filtered to find patterns like names or dates related to possible money launderers.



Search Items	Hits	Files
*.csv	30	8
Edward Talbot	6	3
Patrick Goose	10	4
Mary Shelly	2	1
Charles Darwin	10	2
Daniel Silverman	12	4
Kevin Simmons	2	1
Monica Lopez	2	1
Calvin Moore	2	1
---------------	----	----
Cumulative Results (using OR)	76	8

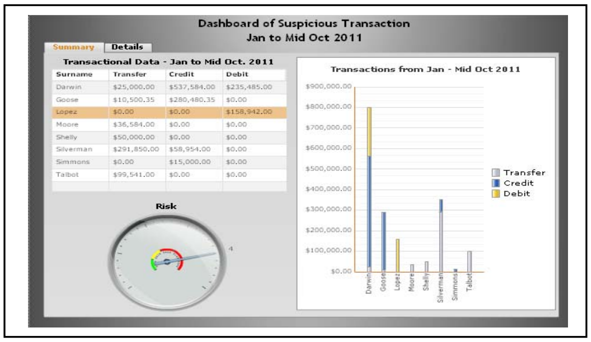
Figure 4. Filtering CSV database logs in FTK

As shown in Fig. 4., the imaged database logs can be used to identify one or various money laundering suspects in order to create more accurate 'SARs', reducing their error rates when using statistical analysis [5].

b) Data Presentation: Once the particular patterns have been extracted from the database logs, the names, transaction amount, etc. can be used to define the approach for data presentation.

Hence, if a statistical approach is used to generate 'SARs', an appropriate data analysis tool can be chosen to create and present an accurate and understandable report [22].E.g. Business Intelligence tools, which in this example is *SAP Crystal Dashboard Designer* (Fig. 5).

[4] *Extract, transform and load (ETL)* is a process in data warehousing to extract information from operational or archive systems, transforming it to meet business needs, and loading it into the end target [30]



Dashboard of Suspicious Transaction
Jan to Mid Oct 2011

Summary | Details

Transactional Data - Jan to Mid Oct. 2011

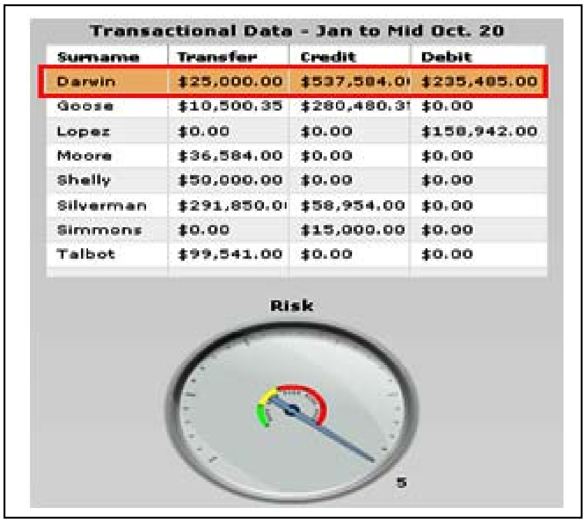
Surname	Transfer	Credit	Debit
Darwin	$25,000.00	$537,584.00	$235,485.00
Goose	$10,500.35	$280,480.35	$0.00
Lopez	$0.00	$0.00	$158,942.00
Moore	$36,584.00	$0.00	$0.00
Shelly	$50,000.00	$0.00	$0.00
Silverman	$291,850.00	$58,954.00	$0.00
Simmons	$0.00	$15,000.00	$0.00
Talbot	$99,541.00	$0.00	$0.00

Figure 5. Dashboard of Suspicious Money Laundering Transactions

In Fig. 5, the CSV files have been exported to a MS Excel file in order to be analysed using BI tools to show the forensic analysis results in a more comprehensive way than using traditional SARs.

C. After the Incident: Case Reporting

If statistical approaches are used to report suspicious activities, 'SARs' can be enhanced to support the investigation using business intelligence (BI). Since data mining techniques can be an important contribution for any digital forensic analysis [2], the current research has considered BI tools as an important approach to deliver SARs by linking the recovered evidence with the money launderers to avoid using extensive written reports. Furthermore, a dashboard has been developed to explain the results during this 'illustrative money laundering case'. For example, in Fig. 6, the customer named 'Charles Darwin' has a high risk of being involved in money laundering activities due to the huge amount of his transactions.



Transactional Data - Jan to Mid Oct. 20

Surname	Transfer	Credit	Debit
Darwin	$25,000.00	$537,584.0	$235,485.00
Goose	$10,500.35	$280,480.3	$0.00
Lopez	$0.00	$0.00	$158,942.00
Moore	$36,584.00	$0.00	$0.00
Shelly	$50,000.00	$0.00	$0.00
Silverman	$291,850.0	$58,954.00	$0.00
Simmons	$0.00	$15,000.00	$0.00
Talbot	$99,541.00	$0.00	$0.00

Figure 6. Suspicious transactions performed by Charles Darwin from January to mid October 2011

V. Conclusion

Previous research [18] showed that anti-money laundering detection models have been developed by financial institutions, but some issues in adopting digital forensics practices inside organisations have made it difficult to enhance them; in particular, due to the over reliance on specialized anti-money laundering tools, and the cost of personnel training in digital forensic practices.

Alternatively, the model presented in this article proposes discovering financial fraud by using databases and forensic tools like FTK, emphasizing data mining and data warehousing techniques to assist digital forensic investigations related to money laundering in compliance with the *Know-Your-Customer 'KYC' policies* defined inside an organisation. Also, this research has proved that BI tools can support the analysis of money laundering evidence using simple database transactional logs in order to present the investigation results in a more comprehensive manner than using extensive written *Suspicious Activity Reports 'SARs'*.

Finally, unlike file systems, database records cannot be compared using MD5 checksums to verify their authenticity [26]; however, this research has shown that obtaining a logical image of specific pre-configured database logs can be considered authentic due to the fact that the MD5 checksum obtained during the imaging stage can validate that these database logs were imaged without manipulating the server's drive, following the principle 1 of the ACPO guidelines [20] and the requirements for relevance, sufficiency, and repeatability of electronic evidence in the BS ISO/IEC 27037 (DIS) standard [27].

Acknowledgment

We wish to acknowledge the sponsorship of the National Secretariat of Higher Education, Science, Technology, and Innovation of Ecuador which have made it possible to undertake this research.

References

[1] V. H. Bhat, P. G. Rao, A. R. V and L. M. Patnaik, "A Novel Data Generation Approach for Digital Forensic Application in Data Mining," in *Second International Conference on Machine Learning and Computing*, 12-13 February. Bangalore, India, 2010.

[2] G. Palmer, "A Road Map for Digital Forensic Research," 6 November 2001. [Online]. Available: http://www.dfrws.org/2001/dfrws-rm-final.pdf. [Accessed 21 April 2012].

[3] N. A. Le Khac and M.-T. Kechadi, "Application of Data Mining for Anti-Money Laundering Detection: A Case Study," in *IEEE International Conference on Data Mining Workshops*, 14 December. Sydney, Australia, 2010.

[4] FATF, "FATF 40 Recommendations (incorporating all subsequent amendments until October 2004)," October 2003. [Online]. Available: http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF. [Accessed 11 February 2012].

[5] R. Hankins, U. Tetsutaroh and L. Jigang, "A Comparative Study of Forensic Science and Computer Forensics," in *Third IEEE International Conference on Secure Software Integration and Reliability Improvement*, 8-10 July. Shanghai, China, 2009.

[6] C. Wright, "SANS Blog: Forensics and Data Access Auditing," 15 March 2009a. [Online]. Available: http://computer-forensics.sans.org/blog/2009/03/15/forensics-and-data-access-auditing. [Accessed 21 April 2012].

[7] K. E. Pavlou and R. T. Snodgrass, "Forensic Analysis of Database Tampering," *ACM Transactions,* vol. 33, no. 4, pp. 30:1 - 30:47, 2008.

[8] FATF, "FATF IX: Special Recommendations (Incorporating all subsequent amendments until February 2008)," October 2001. [Online]. Available: http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf. [Accessed 13 February 2012].

[9] J. Zhang and L. Wang, "Application of Case-oriented Evidence Mining in Forensic Computing," in *International Conference on Multimedia Information Networking and Security*, 18-20 November. hubei, China, 2009.

[10] P. Stahlberg, G. Miklau and B. N. Levine, "Threats to Privacy in the Forensic Analysis of Database Systems," in *ACM International Conference on Management of Data*, 11-14 June. Beijing, China, 2007.

[11] FATF, "Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations (Updated as of February 2009)," 24 February 2004. [Online]. Available: http://www.fatf-gafi.org/dataoecd/16/54/40339628.pdf. [Accessed 20 February 2012].

[12] M. I. Cohen, D. Bilby and G. Caronni, "Distributed forensics and incident response in the enterprise," *Elsevier Digital Investigation: The International Journal of Digital Forensics & Incident Response,* vol. 8, pp. S101-S110, 2011.

[13] J. Haggerty, M. Taylor and D. Gresty, "Determining Culpability in Investigations of Malicious E-Mail Dissemination within the Organisation," in *Third International Annual Workshop on Digital Forensics and Incident Analysis*, 9 October. Malaga, Spain, 2008.

[14] C. Grobler, C. Louwrens and S. Von Solms, "A framework to guide the implementation of Proactive Digital Forensics in Organizations," in *International Conference on Availability, Reliability and Security*, 15-18 February. Krakow, Poland, 2010.

[15] F. Cohen, "Two models of digital forensic examination," in *Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, 21 May. Oakland, US, 2009.

[16] L. Volonino and I. Redpath, "Knowing Why E-Discovery Is a Burning Issue," in *E-Discovery for Dummies*, Hoboken, US, Wiley Publishing Inc., 2010, pp. 9-11.

[17] X. Liu and P. Zhang, "Research on Constraints in Anti-money Laundering (AML) Business Process in China Based on Theory of Constraints," in *41st Hawaii International Conference on System Sciences*, 7-10 January. Hawaii, US, 2008.

[18] X. Liu and P. Zhang, "A scan statistics based Suspicious transactions detection model for Anti-Money Laundering (AML) in financial institutions," in *International Conference on Multimedia Communications*, 7-8 August. Hong Kong, China, 2010.

[19] A. Jansen, "Digital Records Forensics: Ensuring Authenticity and Trustworthiness of Evidence Over Time," in *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering*, 10 May. Oakland, US, 2010.

[20] ACPO - Association of Chief Police Officers, "Good Practice Guide for Computer-Based Electronic Evidence," 2011. [Online]. Available: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. [Accessed 21 April 2012].

[21] P. Frühwirt, M. Huber, M. Mulazzani and E. R. Weippl, "InnoDB Database Forensics," in *24th IEEE International Conference on Advanced Information Networking and Applications*, 20-23 April. Perth, Australia, 2010.

[22] P. K. Panigrahi, "A Framework for Discovering Internal Financial Fraud using Analytics," in *International Conference on Communication Systems and Network Technologies*, 19-21 October. San Francisco, US, 2011.

[23] C. Wright, "SANS Blog: SQL, Databases and Forensics," 11 March 2009b. [Online]. Available: http://computer-forensics.sans.org/blog/2009/03/11/sql-databases-and-forensics. [Accessed 21 April 2012].

[24] P. Kieseberg, S. Schrittwieser, M. Mulazzani, M. Huber and E. Weippl, "Trees Cannot Lie: Using Data Structures for Forensics Purposes," in *European Intelligence and Security Informatics Conference*, 12-14 September. Athens, Greece, 2011.

[25] Computer Database, "Security Information Management Software filters and prioritizes data," 18 March 2011. [Online]. Available: http://go.galegroup.com. [Accessed 21 April 2012].

[26] M. S. Olivier, "On metadata context in Database Forensics," *Elsevier Digital Investigation: The International Journal of Digital Forensics & Incident Response,* vol. 5, pp. 115-123, 2009.

[27] BS ISO/IEC, "27037 Information Technology-Security Techniques-Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence-Draft International Standard (DIS)," 8 November 2011b. [Online]. Available: https://bsol.bsigroup.com/. [Accessed 14 March 2012].

[28] SOCA - Serious Organised Crime Agency, "What is the Financial Intelligence Unit?," 2012. [Online]. Available: http://www.soca.gov.uk/about-soca/the-uk-financial-intelligence-unit. [Accessed 16 May 2012].

[29] Y. Pinto, "A Framework for Systematic Database Denormalization," *Global Journal of Computer Science and Technology,* vol. 9, no. 4, pp. 44-52, 2009.

[30] ETL-Tools-Info, "Definitions and Concepts of the ETL Process," 2012. [Online]. Available: http://etl-tools.info/en/bi/etl_process.htm. [Accessed 16 May 2012].

[31] FATF, "Financial Action Task Force," 2012. [Online]. Available: http://www.fatf-gafi.org/pages/aboutus/. [Accessed 21 May 2012].