DE GRUYTER OPEN

THE EUROPEAN JOURNAL OF APPLIED ECONOMICS

EJAE 2016, 13(2): 45-56
ISSN 2406-2588
UDK: 343.53:657.92
657.632
DOI: 10.5937/ejae13-10509
Review paper/Pregledni naučni rad

FORENSIC ACCOUNTING IN THE FRAUD AUDITING CASE

Nataša Simeunović[1,*], Gojko Grubor[2], Nenad Ristić[1]

[1]University Sinergija,
Str. Raje Baničića bb, Bijeljina, Bosnia and Herzegovina

[2] Singidunum University,
32 Danijelova Street, Belgrade, Serbia

Abstract:
This paper presents a real case of digital forensic analysis in organizational fraud auditing process investigated using two different forensic tools, namely Tableau TD3 Touch Screen Forensic Imager and Access Data FTK Imager. Fraud auditing is more of a mindset than a methodology and has different approaches from financial auditing. Fraud auditors are mostly focused on exceptions, accounting irregularities, and patterns of their conduct. Financial auditors place special emphasis on the audit trail and material misstatements. A fraud case investigation of non-cash misappropriations committed by an employee, the warehouseman, will be presented herein in order to highlight the usefulness of fraud auditing, which can reveal many forms of financial crime and can be used in both private and public sector companies. Due to the computerized accounting environment, fraud investigation requires a combination of auditing, computer crime and digital forensic investigation skills, which can be achieved through joint efforts and cooperation of both digital investigator and fraud auditor as proposed herein.

Key words:
auditing,
accounting,
fraud,
forensic evidence,
digital forensic analysis.

INTRODUCTION

Auditing is a process that enables determining reliability of recorded, classified and summarized financial data. It is necessary due to huge volume of business transactions (IBM, 2013) and complex accounting standards. Accounting differs from auditing, as a process of recording, classification and summarizing of economic events to help the management make informed decisions based on the sound financial data (Nigrini, 2011).

Fraud, as a criminal offence, is a generic term that includes surprising, tricking, cunning, and unfair behaviour by which someone else is cheated. The only boundaries defining it are those that limit human ingenuity to get an advantage through false means or representations. Corporate fraud is any fraud perpetrated by, for, or against some business corporation (Singleton & Singleton, 2010). An occupational fraud and abuse, or employee fraud is: "the use of one's occupation for personal gain through deliberate misuse or theft of the employing

* E-mail: nsimeunovic@sinergija.edu.ba

organization's resources or assets" (Nigrini, 2011). Occupational fraud includes corruption, asset misappropriation and financial statement fraud. The typical organization's loses due to occupational fraud are estimated up to 5% of its annual revenues (ACFE, 2016). In this paper, a fraud case of non-cash misappropriations is presented. An employee steals inventory from the warehouse in order to sell it and earn extra money.

Economic motives are the most common reason for committing despite the presence of other reasons such as egocentric, ideological, emotional *etc*. Essentially, every fraud includes motivation, opportunity and rationalization (the "fraud triangle") (Nigrini, 2011). Many researchers have demonstrated that the fraud triangle can be of great help in profiling employees committing fraud (Seward, 2011). In the computerized accounting environment, fraud could be committed at the input, throughput or output processing phases. However, entering fraudulent data at the input state is the most usual fraudulent behaviour by ordinary employees, including account payables, benefits, or expense claims. Frauds within organizations are mainly associated with the absence of internal controls rather than their weaknesses (Singleton & Singleton, 2010). The lack of internal control starts from the strength of access control mechanism to computers in the business information system. It is well-known that many passwords selected by users can be easily cracked by the so called dictionary attack, even with a laptop and Windows XP operative system within a few seconds. As the password remains the first and the most important authentication method, companies have to devote particular attention to this field. Some international standard recommendations are to select a password with eight or more combined characters (lower and upper case letters, digits and punctuation marks, or other special characters). The length of the user-selected password seems to be a more important parameter. User-selected passwords can provide strong protection if some simple rules are applied and the password encoding hash algorithm of the operating system is strong. The simple rules for a "good" password could be as follows: easy-to-remember, hard-to-guess, in unusual language, rather long, regularly changed, not shared with anybody, and without excessively complex structure (Keszthelyi, 2013).

However, some sophisticated attacks such as Trojan horse key logger installed into a computer can easily steal any user-selected password online. Therefore, accounting frauds can rather be discovered by reactive than proactive measures. Some statistical data show that out of the overall 65% of detected frauds, only 10% are detected by financial auditors, while 23% of frauds are identified by means of proactive internal control measures. Proactive fraud prevention depends mainly on adequate controls and the appropriate workplace culture including a high level of personal honesty and fair behaviour (Nigrini, 2011).

All kinds of fraud such as theft, irregularities, white-collar crime, and embezzlement are almost synonymous, but are not identical in terms of criminal law. In a legal fraud investigation, the intent is the most difficult aspect to be proved, because it occurs in one's mind and the proof is becoming circumstantial. In the private sector, auditing fraud can be useful for most cases of financial crime such as: embezzlement; misrepresentations of financial facts; arson-for-profit; bankruptcy fraud; investment frauds of all manner and deception; bank fraud; kickbacks and commercial bribery; computer frauds; frauds of electronic funds transfer (EFT) systems; credit card frauds; and scams and schemes by vendors, suppliers, contractors and customers. In any and all cases, fraud must be considered an economic, social and organizational phenomenon (Singleton & Singleton, 2010). Therefore, modern organizations need to have a forensically ready cloud environment to respond adequately to forensic events and demonstrate compliance with the applicable laws and regulations (Elyas *et al*., 2014).

In this fraud case, the internal auditor could not detect any irregularities, but remained suspicious due to his business experience and previous

knowledge that the related item was not needed in such quantity. Therefore, he took the case over to digital forensic examiner. In this paper, the aspects of the digital forensic investigation and analysis of the case are described.

REVIEW OF SOME PREVIOUS WORK

Numerous authors have already elaborated on the methods and techniques of forensic accounting investigations. According to Nigrini, forensic accounting investigation process is described in detail. Some advanced techniques such as data mining (Panigrahi, 2006) and mathematical models (Panigrahi, 2006; Nigrini, 2009) have also been suggested for the forensic accounting investigations process. As regards financial statement audits, the most frequently used tools for examination of client data are Excel, CaseWare IDEA and ACL Software. Traditionally, these and similar tools have been called Computer Assisted Audit Tools and Techniques - CAATTs (Coderre, 2009). Some specific data mining tools can disclose patterns of fraudulent data transactions such as unusual entries of transactions, excessively high or low value of a variable, and various files of accounting transactions or unexplained values of records. Gray & Debreceny (2014) identified specific fraud and evidence combinations in which the use of data mining would be the most or least effective. By taking into consideration fraud scheme components defined by Gao and Srivastava (2011) and data mining functionality, they proposed a taxonomy that identifies the most effective combinations of those components. Although there isn't much information in the literature on the application of data mining techniques to auditing in general and fraud detection in particular, some sources need to be mentioned (Jans *et al.*, 2010; Ravisankar *et al.*, 2011; Perols, 2011; Alden *et al.,* 2012). The first mathematical model (The Benford's Law) suggested that fraudulent figures have a different pattern than the valid ones, while the second model (The Relative Size Factor) detects unusual figures and data that could be made by errors or frauds (Panigrahi, 2006). However, the growth of big data and belonging technology (IBM, 2013), and the complexity of financial transactions and fraudsters' skilfulness are the main problems in forensic accounting and fraud investigation processes.

DIGITAL FORENSIC INVESTIGATION IN FRAUD AUDITING PROCESS

Digital forensic investigation, by its nature, is a dichotomy phenomenon; it is as much an art as it is a science. At the same time, it represents both an intuitive process and the formal analytical and scientific methodology (Milosavljević & Grubor, 2010). Therefore, it is difficult to be taught and learned. Similarly, fraud auditing process depends more on intuition and thinking as a thief would, than on various formally learnt subjects. A digital forensic examiner, like a fraud auditor, looks for relevant information without presumption, organizes it and tries to discover relevant data and make a pattern they create in order to reconstruct what may have occurred (Singleton & Singleton, 2010; Milosavljević & Grubor, 2010). Event reconstruction is one of the most important steps in digital investigation. It allows investigators to understand the timeline of a criminal case (Chabot *et al.*, 2014). Also, in the computerized environment, fraud auditors should be familiar with relevant legislation, applicable standards and other requirements within the organization.

However, investigating fraud related to computers or networks as well as the Internet requires a combination of auditing, computer crime and digital forensic investigation skills. In the current reporting environment, forensic accountants are undoubtedly in great demand for their accounting, auditing, legal, and investigative skills. They can play a vital role in coordinating the company's efforts to achieve a cohesive policy of ethical behaviour within an organization (Bhasin, 2015; Arežina *et al.*, 2014; Gbegi & Adebisi, 2014). Unfortunately, it is quite difficult to encounter all these skills in one person. A digital forensic investigator applies forensic rules, principles, techniques and tools to

investigate the computer related fraud (Harlan, 2009; Jones *et al.*, 2005). On the other hand, auditors could provide forensic investigators with the knowledge of accounting and auditing rules, principles, techniques, and methods. Since generic fraud involves many variables such as fraud types, victim types, crime methods, techniques and tools, it seems almost impossible to create a unified and comprehensive theory or solution.

Hence, a model of combined approach and team work of both digital investigator and fraud auditor is proposed herein. However, a digital forensic examiner should be familiar with the main principles of fraud audit to be effective in fraud investigation (Table 1) (Singleton & Singleton, 2010).

No.	Fraud auditing principle
1	Being at the same time an art and a science, fraud auditing is different from financial auditing.
2	Fraud auditors place emphasis on the exceptions, irregularities, and oddities of accounting conduct patterns.
3	Essentially, any fraud is an intentional change of financial or material facts in order to gain some benefits.
4	Despite some fraud theories, fraud auditing is learned primarily from experience.
5	There are many reasons for committing fraud such as economic, emotional, egocentric, psychotics *etc*.
6	Places where fraud could be committed in digital environment are at input, transition or output of transaction.
7	Some financial gains are the most usual among internal frauds made by employees.
8	The lack of or poor control is most often the cause of accounting frauds.
9	Accounting frauds are more often discovered by reactive than proactive actions.
10	Proactive fraud measures mainly depend on adequate internal controls, personal honesty and fair business.

Table 1. The main principles of fraud auditing

The inventory oversize is the most common type of organisational fraud. The number of purchased items is more or less susceptible to fraud, and is therefore necessary to check and correct the data in the orders and on the invoices. This is a rather simple process as it does not require illegal transactions (Kwok, 2008). However, stealing material items from the company is almost always a result of false data disclosed in financial reports and can be easily hidden in the computer system.

In the case of organisational fraud, the main objective is to determine whether a fraud has occurred, or is occurring, and identify the fraudster. The first step is to make a hypothesis in order to initiate fraud investigation. According to digital forensic science, the forensic hypothesis must have at least six elements (Milosavljević & Grubor, 2010), but eliminating all of the obvious facts is the very first one. Forensic investigator should prove whether the fraud has already happened or is happening, or will happen. Afterwards, the forensic investigator should generate most likely fraud scheme and propose it to the fraud auditor. Fraud investigation plan in digital environment should include data collection, acquisition, analysis and digital evidence presentation, as well as the choice of the appropriate forensic tools and techniques. Forensic investigator and fraud accountant must maintain a chain of custody of forensic evidence and preserve evidence integrity until the end of the legal process (Jones *et al.*, 2005; Kwok, 2008). At the end of fraud reconstruction, the forensic investigator and fraud accountant write up their findings for hiring party and courtroom.

Upon gathering accounting evidence from the computer system and network, the forensic accountant (or fraud accountant) will attempt to gather evidence from other sources such as the crime investigator, video monitoring system and eyewitnesses, in order to reconstruct the fraud event. In the next step, the forensic accountant mounts a forensic image of the suspected computer and other relevant data from the investigation process onto the virtual forensic machine

to prevent the so-called "Trojan Horse Defence" (Milosavljević & Grubor, 2010), and prove the suspect's knowledge or unawareness. Immediately upon that, a forensic analyst or forensic accountant analyses the traces of the acquired corroborative digital data and the data from other sources, such as video monitoring system or law enforcement information, using the appropriate forensic tools and techniques (Harlan, 2009; Milosavljević & Grubor, 2010). The digital evidence can be a key to reconstruct any fraud in digital environment and to create report and perform courtroom testimony (Winch, 2007). In this fraud case, the Integrated Forensic Accounting Process Model (Grubor *et al*., 2013) is applied by two digital forensic analysts (DFAs) using two different forensic tools. However, a professional accountant had to interpret the content of the digital evidence findings (AFTWIT).

FRAUD CASE - FORENSIC ANALYSIS

In this fraud case, the senior accountant from the inventory team, getting suspicious about the unusual excess of the subject item, made the first step in the investigation process. He collected the data from video monitoring system and acquired the suspected computer as electronic evidence. However, he couldn't prove his suspicions due to the lack of digital forensic knowledge. Thereafter, he hired a DFA who took forensic image of the suspected computer's hard disk. In order to verify the digital evidence, two forensic analysts from the Association (AFTWIT) performed an independent analysis using two different forensic tools (Figure 1).

The forensic analysts worked separately but interactively with the senior accountant on the main decision points. Finally, the DFAs and the

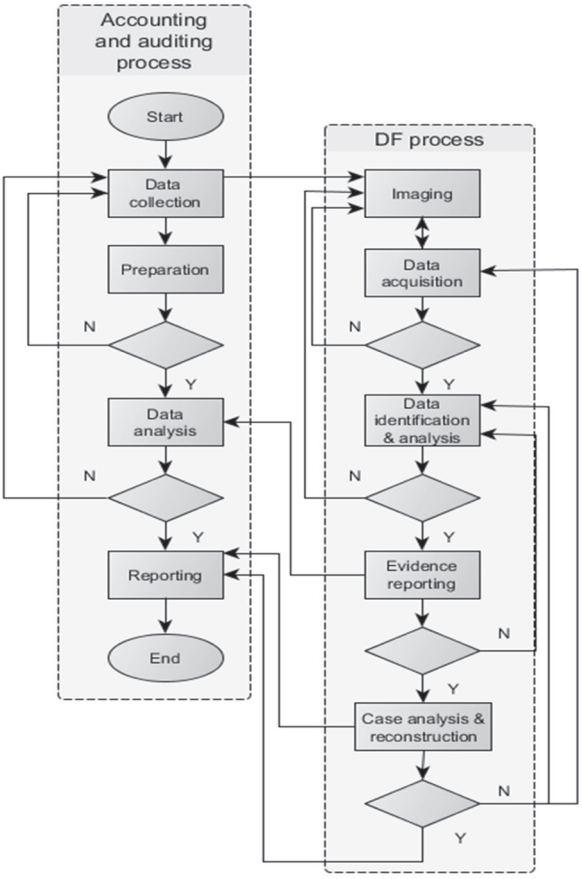

Figure 1. Integrated forensic accounting investigative process model
Source: Grubor et al. (2013)

accountant jointly reconstructed the fraud case and reported findings to the company's owner who was supposed to give over the case to the law enforcement (Grubor *et al*., 2013).

The senior accountant, as an internal auditor, described fraud event in his investigation requirement (Table 2). The DFA, hired by the Association (AFTWIT), received the compromised computer with user accounts and passwords.

Warehouseman was informed on Friday afternoon that part-time inventory started on Monday morning.
On Friday afternoon, the accountant printed the list of inventory to the internal auditors team.
On Monday morning, the accountant gave the list of inventory to the internal auditors' team.
Auditors identified that there were 134 pieces of article under code number 1034.
A member of auditing team from purchasing department got suspicious regarding the quantity of item 1034.
A leading internal auditor required printing of item 1034 card and identified only 74 pieces.
An accountant printed again the inventory report from the ledger and there were 74 pieces of the article 1034 in it.

Table 2. Requirements for forensic investigation

As the first step, the forensic analysts identified the following facts:

1. Compromised computer was turned off and the printer was not logged in the history of usage.
2. The computer was neither networked nor the member of any domain.
3. Controversial reports had been printed via the USB device.
4. Computer had wireless Internet access, antivirus program and firewall.
5. There was no cryptography in the computer.
6. Hard disk (HD) was 120 GB, Operative system was XP Professional SP3.
7. Accountant, warehouseman, seller, system administrator, accounting application administrator, owner and internal auditor were familiar with the user account and password to log in OS and accounting application.

Afterwards, the forensic analyst took forensic image of HD 120 GB (Table 3) locally by *Tableau TD3 Touch Screen Forensic Imager* in order to investigate the accounting application in a virtual machine.

Physical Evidentiary Item (Source) Information	
[Drive Geometry]	
Cylinders:	14,593
Tracks per Cylinder:	255
Sectors per Track:	63
Bytes per Sector:	512
Sector Count:	234,441,648
[Physical Drive Information]	
Drive Model:	TOSHIBA MK1252GSX
Drive Serial Number:	948TLO2TC
Drive Interface Type:	IDE
Source data size:	114473 MB
Sector count:	234441648
[Computed Hashes]	
MD5 checksum:	e1533bfc695ae563f-c9302a37e4d8786
SHA1 checksum:	2ce5cadc0ca54d-82ce21924e0498448536b23505

Table 3. Forensic image data

In the next step, a virtual machine is created by *Live View 07b* forensic open source tool. Then, Windows OS (Harlan, 2009) event log, recent programs, recent items and hidden data (Keman, 2004), as well as the accounting application metadata (Jones, 2006; Microsoft KB, 2007; Microsoft

KB, 2013) are analysed. *The RegScanner* program is installed to identify changes in Registry key from Friday (June 21, 2013) to Monday (June 24, 2013). The image analysis results on the forensic virtual machine from June 24, 2013 at 08:19:45 AM up to June 24, 2013 at 08:37:13AM are summarized in Table 4.

1. In Registry base are identified:
a. use of accounting application Prvi2005.exe b. access to .pdf document - report "inventory report 2013.pdf", created at Friday c. access to .pdf document - report "part-time inventory report 2013.pdf", created at Sunday
2. Comparison of the two reports (from Friday and Sunday) shows:
a. State of item 1034 in ledger list was increased for 60 pieces in report "part-time inventory report 2013.pdf".

Table 4. The results of image analysis on the forensic virtual machine

The digital evidence retrieved by the *RegScanner* analysis of the events from June 24, 2013 at 08:19:45AM up to June 24, 2013 at 08:37:13AM, in Microsoft (MS) *Access* data base, use of Adobe. *pdf* file and accountant application are shown in Tables 5, 6 and 7, respectively.

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Access\Place MRU
HKEY_USERS\S-1-5-21-527500354-3516707547-4227690221-1000\Software\Microsoft\Office\15.0\Access\Place MRU
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Access\File MRU
HKEY_USERS \S-1-5-21-527500354-3516707547-4227690221-1000\ Software\Microsoft\Office\15.0\ Access\File MRU
HKU \S-1-5-21-527500354-3516707547-4227690221-1000\ Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mdb

Table 5. The evidence from MS Access data base

The evidence from the use of Adobe *.pdf* document is shown in Table 6.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
HKU \S-1-5-21-3847162342-2421605019-2411098501-1006\ Software\Adobe\AcrobatReader\8.0\AVGeneral\cRecentFiles\c2
HKU \S-1-5-21-3847162342-2421605019-2411098501-1006\ Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Table 6. The evidence from the Adobe .pdf document

The evidence for the use of accountant application is presented in Table 7.

HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\RunMRU

Table 7. The evidence for the use of accountant application

The results of the system log file analysis are shown in Tables 8 and 9, respectively.

Log Name:	System
Source:	Microsoft-Windows-Kernel-General
Date:	24.6.2013 8:19:45
Event ID:	12
Task Category:	None
Level:	Information
Keywords:	
User:	kosa
Computer:	Toshiba
Description:	The operating system started at system time 2013-06-24,08:19:45.375199800.

Table 8. Event log "12"evidence for computer turning on (June 24, 2013 at 08:19:45AM)

Log Name:	System
Source:	Microsoft-Windows-Kernel-General
Date:	24.6.2013 08:37:13
Event ID:	13
Task Category:	None
Level:	Information
Keywords:	N/A
User:	N/A
Computer:	Toshiba
Description:	The operating system was shutting down at system time 2013-06-24,08:37:13.673632100.

Table 9. Event log "13" evidence for computer turning off (June 24, 2013 at 08:37:13AM)

The results of the file system forensic analysis are obtained by opening HD image in Access Data FTK Imager forensic tool (Table 10).

In MS Access base file "GSD2013.mdb" is modified on June 24, 2013 at 08:23:14h
.pdf part-time inventory report ("izvestajzapopisvanredni 2013.pdf") is on created June 24, 2013 at 08:23:14h
.pdf part-time inventory report ("izvestajzapopisvanredni2013.pdf") is accessed on June 24, 2013 at 08:24:51h
Accountant application "Prvi2005.exe" is used on June 24, 2013 at 08:26:33h

Table 10. The results of RegScanner analysis by Access Data FTK Imager

RESULTS OF FORENSIC ANALYSIS

Forensic analysts produce a forensic report (King, 2009), including their opinions and recommendations. In this fraud case, somebody under the user name "*Kosa*" used the computer with accounting application and financial data of the company between June 24, 2013 at 08:19:45AM and June 24, 2013 at 08:37:13AM. The MS Access data base "*GSD2013.mdb*" was changed and accounting application "*Prvi2005.exe*" was used. It was proved that there were two versions of the inventory report from the ledger list – one from Friday and the other one from Sunday. In the report from Sunday, there were 60 pieces of the item No. 1034, which is more than in the previous one.

It was necessary to identify who visited the office on Sunday 24, June 2013, and whether he/she knew the credentials for the access to the computer and accounting application, and to investigate his/her motives for such manipulation.

FRAUD CASE RECONSTRUCTION

According to the results of the digital forensic analysis and evidence from other sources such as records of video monitoring system and internal accounting auditor's investigation, the fraud case was reconstructed by team work comprising an internal accounting auditor and two digital forensic analysts. The warehouseman N.M. made a secret deal with the supplier in order to make and share some extra money. Thus, alongside the regular order, he received some extra items from the supplier which he later on traded on the black market for cash. He was supposed to share all extra money earned with the supplier. He never made a record of those extra items in the financial documents and books, nor presented them as the company's trade business. The suspected item is stored under the code No. 1034 in the inventory and financial database. In the warehouse, there were 60 pieces of that item unrecorded in the company's official documents and item cards. However, the general manager of the company suddenly ordered an internal control of inventories due to some other operational reasons. Therefore, the warehouseman did not have sufficient time or the opportunity to remove the extra stocked items. In order to deceive the internal auditing team by claiming that there was no higher number of the item No. 1034 recorded in books, the warehouseman committed the following deception. He had already known that the company's accountant printed out the inventory list with the registered amount of 74

pieces of the item No. 1034 instead of 134, and left it on his table on Friday afternoon with the intention of giving it over to the internal auditing team after finishing inventory of the stored items on Monday morning. Hence, the warehouseman came to the company on Sunday, with an excuse that he was preparing the warehouse for inventory registration. However, he quietly slipped into the office of an accountant and printed out a new, false inventory list with the amount of 134 pieces of the item No. 1034, and replaced it with the correct list that had already been on the table. He also accessed the database and changed the amount of the same item in the entering documents. Instead of 74 pieces of the ordered item No. 1034 and its value of 11,680 RSD, he changed them to 134 pieces with the value of 29,200 RSD. Since he knew the password, he opened the accounting software and changed the same values. He printed out a false report and replaced already completed report on the table made by the accountant of the company on Friday afternoon. Thereafter, warehouseman accessed the database and returned the replaced data back to correct values (74 and 11,680 RSD). On Monday morning, the accountant of a company took the report from his table, unaware that it was a false one, and gave it to the internal auditing team. Hence, the auditors were able to discover "the right state" in the stored items, and the warehouseman still had extra items to sell for profit.

However, a member of the inventory team became suspicious about such high number of item No. 1034, since he had experience with that item from his previous job in the same company.

Therefore, he decided to check it with the commercial department and ask them why they purchased so many pieces of item No. 1034. In fact, that was the red flag for the main accountant to start his investigation. Having certain difficulties to understand changes in commercial documents and compare database, he decided to hire the forensic investigator from the Association of Forensic Testimony Witnesses for Information Technology in the Republic of Serbia (AFTWIT).The hired forensic investigator employed another forensic analyst from the Association, just to confirm the digital evidence through two independent analyses and different forensic tools.

It could be observed from the video monitoring system that only one person visited the office of the chief accountant during the weekend. This reduced the number of suspects to one person. In spite of the completed fraud investigation, there was not sufficient evidence to confirm that a particular person committed fraud. However, using digital evidence from the digital forensic analysis process, it was confirmed that the suspected warehouseman committed the fraud.

Generally, four kinds of evidence are commonly used for fraud prosecution: physical evidence, evidence based on witness testimony, documentary evidence and demonstrative evidence (Kwok, 2008). In this fraud case, the documentary evidence supported by demonstrative digital forensic evidence was prepared for a likely legal procedure. Fraudsters sometimes use false documents to cover up the fraud. Obviously, this fraud could be unlikely discovered only based on the false financial documents. In this case, besides false documents, the digital traces made by the company's computer and video monitoring systems were more decisive for fraud reconstruction.

From the digital forensic point of view, in order to prevent such kind of fraud through computer misuse and change of the accounting application, the option Track Changes in reporting Excel file must have been enabled and another application implemented to prevent its disabling (Microsoft KB, 2007). In this way, all changes would be recorded in Excel metadata and forensic investigation would be easier.

The need for quite a new approach to security of the company's information asset (information, physical and human) (ISO, 2013) can be the first lesson learnt from this fraud case. Obviously, to prevent internal fraud in digital environment, a comprehensive micro-risk assessment must be performed more often than recommended by nu-

merous international standards and recommendations (once or twice per year). A complex, *holistic business enterprise security model* suggested by the authors in the reference (Michelberger & Lábodi, 2012), including risk-adopted access control mechanism that can deal with real-time threats and layered managing, operational and technical security controls (ISO, 2013; National Institute for Standards and Technology, 2013), should be applied to any business information system to prevent or efficiently reduce internal fraud in digital environment. To reduce possible fraudulent activities, the companies can also employ continuous auditing techniques (Chan & Vasarhelyi, 2011; Vasarhelyi *et al*., 2012) in order to manage risk as well as to provide continuous assurance (Vasarhelyi *et al*., 2004).

CONCLUSIONS

Taking into consideration previously explained case study and available literature, it is blatantly obvious that ICTs (Information and communications technologies) play an increasing role in capturing accounting and overall business processes in an organization. It could be observed from the available fraud statistics and relevant history that fraud can occur anywhere and it continues to grow, especially in terms of losses and frequency. Therefore, in order to successfully investigate fraud, joint efforts of both digital investigator and fraud auditor is required by combining their auditing, computer crime and digital forensic investigation skills, which can be hardly encountered in a single person. Both of these two roles, fraud auditing and digital forensics, require skills, knowledge and abilities exceeding the traditional financial auditing.

There are some key aspects of the fraud investigation and many of them can be revealed in digital forensic examination process. In order to effectively and efficiently detect fraud within a short period of time, it is crucial to provide strategic direction of the investigation prior to initiating the fraud analysis in digital environment. As a proactive anti-fraud profession has grown significantly over the last decade (National Institute for Standards and Technology, 2013), anti-forensic activities are also becoming more and more sophisticated in order to hide or destroy digital data traces and potential digital evidence.

In this paper, the authors applied the proposed fraud investigation model in the real fraud case and emphasized the importance of team work of an accounting auditor and digital forensic examiner to efficiently resolve any financial fraud in digital environment. However, continuous monitoring of development and usage of ICTs in capturing business processes in the company is necessary in order to effectively and efficiently adopt and implement the upcoming changes in the fraud investigation process.

One of the ways to fight fraud is to provide forensic readiness of companies in order to ensure a healthy business environment for development of national economies.

REFERENCES

Alden, M.E., Bryan, D.M., Lessley, B.J., & Tripathy, A. (2012). Detection of Financial Statement Fraud Using Evolutionary Algorithms. *Journal of Emerging Technologies in Accounting*, 9(1), 71-94. doi:10.2308/jeta-50390

Arežina, N., Knežević, G., Simeunović, N., & Vukićević, S. (2014). *Forensic Accountant: Innate Trait or Acquired Skill*? Singidunum University International Scientific Conference Financial Reporting Function of the Corporate Governance, Belgrade, December 5 (pp. 131-134). Belgrade: Singidunum University. doi:10.15308/finiz-2014-131-134

Association of Certified Fraud Examiners. (2016). *Report to the Nations, 2016 Global Fraud Study*. Retrieved April 14, 2016, from http://www.acfe.com/rttn2016.aspx

Bhasin, M. (2015). *An Empirical Investigation of the Relevant Skills of Forensic Accountants: Experience of a Enveloping Economy*. Retrieved April 04, 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676519

Chabot, Y., Bertaux, A., Nicolle, C., & Kechadi, M.T. (2014). A Complete Formalized Knowledge Representation Model for Advanced Digital Forensics Timeline Analysis. *Digital Investigation*, 11, S95-S105. doi:10.1016/j.diin.2014.05.009

Chan, D.Y. & Vasarhelyi, M.A. (2011). Innovation and Practice of Continuous Auditing. *International Journal of Accounting Information Systems*, 12(2), 152-160. doi:10.1016/j.accinf.2011.01.001

Coderre, D.G. (2009). *Computer-Aided Fraud Prevention and Detection: A Step-by-Step Guide*. New Jersey: John Wiley & Sons.

Elyas, M., Maynard, S.B., Ahmad, A., & Lonie, A. (2014). Towards a Systemic Framework for Digital Forensic Readiness. *Journal of Computer Information Systems*, 54(3), 97-105. doi:10.1080/08874417.2014.11645708.

Gao, L., & Srivastava, R.P. (2011). The Anatomy of Management Fraud Schemes: Analyses and Implications. *Indian Accounting Review*, 15(1), 1-23.

Gbegi, D.O., & Adebisi, J.F. (2014). Forensic Accounting Skills and Techniques in Fraud Investigation in the Nigerian Public Sector. *Mediterranean Journal of Social Sciences*, 5(3), 243. doi:10.5901/mjss.2014.v5n3p243

Gray, G.L., & Debreceny, R.S. (2014). A taxonomy to Guide Research on the Application of Data Mining to Fraud Detection in Financial Statement Audits. *International Journal of Accounting Information Systems*, 15(4), 357-380. doi:10.1016/j.accinf.2014.05.006

Grubor, G., Ristić, N., & Simeunović, N. (2013). Integrated Forensic Accounting Investigative Process Model in Digital Environment. *International Journal of Scientific and Research Publications*, 3(12), 1-9.

Harlan, C. (2009). Windows Forensic Analysis DVD Toolkit, Ch. 8, p. 411: Syngress Publishing. Inc. Retrieved April 12, 2016, from http://160.216.223.99/vyuka/forensics/Windows%20Forensic%20Analysis%20DVD%20Toolkit%20%20Second%20Edition.pdf

IBM. (2013). *Big Data at the Speed of Business*. Retrieved November 25, 2015, from http://www-01.ibm.com/software/data/bigdata

ISO/IEC 27001. (2013). *Information Technology: Code of Practice for Information Security Management*. Retrieved November 27, 2015, from http://www.iso27001security.com/html/27001.html

ISO/IEC 27002. (2013). *Information Technology: Code of Practice for Security Controls*. Retrieved November 27, 2015, from http://www.iso27001security.com/html/27002.html

Jans, M., Lybaert, N., & Vanhoof, K. (2010). Internal fraud risk reduction: Results of a data mining case study. *International Journal of Accounting Information Systems*, 11(1), 17-41. doi:10.1016/j.accinf.2009.12.004.

Jones, J.R. (2006). *Document Metadata and Computer Forensics.* James Madison University Infosec Techreport, Department of Computer Science. Retrieved January 15, 2016, from http://creative.cisat.jmu.edu/projects/CS/infosec/documents/jmu-infosec-tr-2006-003.pdf

Jones, K.J., Bejtlich, R., & Rose, C.W. (2005). *Real Digital Forensics: Computer Security and Incident Response*. Upper Saddle River, NJ: Addison-Wesley.

Keman, D. (2004). *Hidden Data in Electronic Documents, GIAC GSEC Practical (v.1.4b, Option 1), SANS Institute InfoSec Reading Room.* Retrieved January 25, 2016, from https://www.sans.org/reading-room/whitepapers/privacy/hidden-data-electronic-documents-1455

Keszthelyi, A. (2013). About Passwords. *Acta Polytechnica Hungarica*, 10(6), 99-118. doi:10.12700/APH.10.06.2013.6.6

King, J.R. (2009). *Document Production in Litigation: Use an Excel-Based Control Sheet. National Association of Valuation Analysts*. Retrieved December 19, 2015, from http://www.investopedia.com/terms/n/national-association-of-certified-valuation-analysts.asp

Kwok, B.K.B. (2008). *Forensic Accountancy*. Ohio: LexisNexis.

Michelberger, P., & Lábodi, C. (2012). After Information Security: Before a Paradigm Change (A Complex Enterprise Security Model. *Acta Polytechnica Hungarica*, 9(4), 101-116.

Microsoft Knowledge Base. (2007). *How to minimize metadata in Microsoft Excel Workbooks, Article ID: 223789*. Retrieved January 15, 2016, from http://aumha.org/index.htm

Microsoft Knowledge Base. (2013). *Microsoft Office and Forensic Accounting: Advanced Techniques, Effective Tests, & Valuable Tips for Excel, OneNote, Word, PowerPoint, & Access*. Retrieved January 15, 2016, from http://aumha.org/index.htm.

Milosavljević, M., & Grubor, G. (2009). *Digitalna forenzika računarskog sistema*. Beograd: Univerzitet Singidunum. In Serbian.

Milosavljević, M., & Grubor, G. (2009). *Istraga kompjuterskog kriminala*. Beograd: Univerzitet Singidunum. In Serbian.

National Institute for Standards and Technology. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. doi:10.6028/NIST.SP.800-53r4

Nigrini, M. (2009). *Benford's Law Excel 2007/2010 Software*. Retrieved December 10, 2015, from http://www.nigrini.com/datas_software.htm

Nigrini, M. (2011). *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*. Hoboken, NJ: John Wiley & Sons.

Panigrahi, P.K. (2006). *Discovering Fraud in Forensic Accounting Using Data Mining Techniques. The Chartered Accountant*, April(2006), 1426-1430. Retrieved February 16, 2016, from http://assets.cacharya.com/Discovering-Fraud-in-Forensic-Accounting-Using-Data-Mining-Techniques-Published-MQWQNJHS.pdf?1425861052

Perols, J. (2011). Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms. *Auditing: A Journal of Practice & Theory*, 30(2), 19-50. doi:10.2308/ajpt-50009

Ravisankar, P., Ravi, V., Raghava Rao, G., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems*, 50(2), 491-500. doi:10.1016/j.dss.2010.11.006

Seward, J. (2011). *Forensic Accounting: The Recorded Electronic Data Found on Computer Hard Disk Drives, PDAs and Numerous Other Digital Devices*. Retrieved November 22, 2015, from https://articles.forensicfocus.com/2011/06/27/forensic-accounting-the-recorded-electronic-data-found-on-computer-hard-disk-drives-pdas-and-numerous-other-digital-devices/

Singleton, T.W., & Singleton, A.J. (2010). *Fraud Auditing and Forensic Accounting*. Hoboken, NJ: John Wiley & Sons.

Vasarhelyi, M.A., Alles, M.G., & Kogan, A. (2004). Principles of Analytic Monitoring for Continuous Assurance. *Journal of Emerging Technologies in Accounting*, 1(1), 1-21. doi:10.2308/jeta.2004.1.1.1

Vasarhelyi, M.A., Alles, M.G., Kuenkaikaew, S. & Littley, J. (2012). The Acceptance and Adoption of Continuous Auditing by Internal Auditors: A Micro Analysis.*International Journal of Accounting Information Systems*, 13(3), 267-281. doi:10.1016/j.accinf.2012.06.011

Winch, D. (2007). *Finding and using a forensic accountant*. Retrieved December 5, 2015, from http://www.accountingevidence.com/documents/articles/Forensic%20accountant1.pdf

FORENZIČKO RAČUNOVODSTVO NA PRIMERU SLUČAJA ISTRAŽIVANJA PREVARE

Rezime:

Ovaj rad prikazuje slučaj digitalne forenzičke analize u okviru koje se ispituju prevare izvšene unutar organizacije korišćenjem dva različita alata za forenzičku analizu, Tableau TD3 Touch Screen Forensic Imager i Access Data FTK Imager. Istraživanje prevara je više odraz mentalnog stava, a ne metodologije i ima drugačiji pristup u odnosu na finansijsku reviziju. Revizori se prevashodno bave izuzecima, računovodstvenim nepravilnostima i utvrđivanjem obrazaca njihovog ponašanja. Finansijski revizori obraćaju posebnu pažnju na revizorski trag i materijalno značajne greške. Revizija slučaja bezgotovinskih pronevera izvršenih od strane zaposlenog, magacionera, biće predstavljena u ovom radu kako bi se se istakao značaj procesa ispitivanja prevare koji može ukazati na različite oblike finansijskog kriminala, a može se koristiti u privatnim i državnim preduzećima. Kako bi se utvrdilo prisustvo prevara u kompjuterizovanom računovodstvenom okruženju, neophodno je posedovati znanja i veštine od značaja za proces revizije, kompjuterski kriminal i digitalnu forenzičku istragu, a koja se mogu steći kroz timski rad i saradnju digitalnih istražitelja i finansijskih revizora.

Ključne reči:
revizija,
računovodstvo,
prevara,
forenzički dokaz,
digitalna forenzička analiza.

Received: March 16, 2016
Correction: May 19, 2016
Accepted: May 26, 2016