ISSN 2250-3153

Integrated Forensic Accounting Investigative Process Model in Digital Environment

Gojko Grubor*, Nenad Ristić, Nataša Simeunović*****

*PhD, Assistant professor, Sinergija University, Bijeljina, Bosnia and Herzegovina
ggrubor@sinergija.edu.ba
**Teaching Assistant, PhD student, Sinergija University, Bijeljina, Bosnia and Herzegovina nristic@sinergija.edu.ba
***Teaching Assistant, PhD student, Sinergija University, Bijeljina, Bosnia and Herzegovina nsimeunovic@sinergija.edu.ba

Abstract: *A new field of forensic accounting has emerged as current practices have been changed in electronic business environment and rapidly increasing fraudulent activities. Despite taking many forms, the fraud is usually theft of funds and information or misuse of someone's information assets. As financial frauds prevail in digital environment, accountants are the most helpful people to investigate them. However, forensic accountants in digital environment, usually called fraud investigators or fraud examiners, must be specially trained to investigate and report digital evidences in the courtroom. In this paper, the authors researched the case of financial fraud forensic analysis of the Microsoft Excel file, as it is very often used in financial reporting. We outlined some of the well-known difficulties involved in tracing the fraudster activities throughout extracted Excel file metadata, and applied a different approach from that well-described in classic postmortem computer system forensic analysis or in data mining techniques application. In the forensic examination steps we used open source code, Deft 7.1 (Digital evidence & forensic toolkit) and verified results by the other forensic tools, Meld - a visual diff and merge tool to compare files and directories and KDiff tool, too. We proposed an integrated forensic accounting, functional model as a combined accounting, auditing and digital forensic investigative process. Before this approach can be properly validated some future work needs to be done, too.*

Key words: *fraud, financial accounting, financial fraud, forensic accounting, digital forensic analysis*

1. Introduction

Generally, fraud includes a wide range of illegal activities, mainly based on intentional deception. However, theft of funds or information or misuse of someone's assets that can cause loss of money, clients' confidence and reputation at the market are the most usual. The fraud appears as prevailing *financial* and rather insignificant – *non-financial* one. The financial fraud has become a common phenomenon inside many companies [5]. Most of the financial fraud cases involve some kind of revenue manipulation, e.g. revenue overstatement that is usually occurring in the client's financial books. Companies simply invent revenues, as a credit or debit, producing false balance sheet and income statement [21].

So, an accountant and auditor have to look for this type of fraud throughout the internal control and audit processes. In digital environment context, *forensic accounting* plays an important role in detecting these frauds that are not discovered in accounting and internal auditing process. However, forensic accounting is a great challenge for regular accountants and accounting auditors due to the lack of knowledge and experiences in digital forensic investigation. The main objective of the proposed integrated process model is to promote practical needs for combined work of the accountants, auditors and digital forensic investigators in the complex Internet environment. According to the available literature, at the current market it is quite difficult to find an accountant who is both knowledgeable and experienced in digital forensic investigation and vice versa, as well. In the forensic accounting approach, forensic accounting is sometimes called *forensic analytics*, meaning the analysis of digital data in order to detect, recover and reconstruct them or otherwise support or deny a claim of financial fraud [16]. The main steps in forensic accounting are *data collection, preparation, analysis and reporting* [16, 21]. On the other side, digital forensic investigative process can be defined in many ways, depending on its type of application. However, prevailing definition of public (law enforcement) forensic investigation includes the following steps: *forensic imaging, data acquisition (preparation and extraction), data identification and analysis, reporting, and case analysis* [19]. In this paper the authors proposed an integrated forensic accounting functional process model, which uses a synergy approach of accountants, accounting auditors and digital forensic analysts.

2. Review of some known *financial fraud* and *forensic accounting* approaches

In general, the taxonomy of fraud can be very complex as it can be performed in many ways and appeared in many forms such as crime, corporate fraud, management and occupational fraud, person's dishonesty, *intentional* deception, etc. Therefore, fraud, theft, irregularities, white-collar crime and embezzlement are almost synonyms. The main factors that could initiate someone to commit a fraud include *opportunity*, *rationalization* (or personal justification for doing it) and any kind of *financial pressure* against someone. These factors are well known and defined in the reference [16]. *The financial pressure* can be a certain motive for the fraudster to steal. The *rationalization* describes how fraudsters justify their criminal actions? The *opportunity* can emerge when the perpetrator is in a trusted position somewhere followed by weakness in, or absence of internal controls that provide the circumstances for the fraudster to commit a crime [16].

In regular *financial auditing process*, the focus is on a sample of transactions, accuracy and reliability of the financial statements, and making remark in auditing report in case of any deviation, error, unusual exaggeration, etc. [16]. Some auditing tools, such as CAATs (*Computer Assisted Auditing Tools*) [9], are currently used to deal with big financial data sets, process complex transactions and help auditor with implementing auditing procedures, such as [9, 16]:

a) Testing details of transactions and balances;
b) Identifying inconsistencies and transaction's fluctuations;
c) Sampling programs to extract data for audit testing;
d) Testing general and application control of computer, and
e) Redoing calculations performed by the accounting systems.

The forensic accounting process differs from regular financial auditing, searching only for suspicious transactions, and using a strict digital forensic process [7, 15, 19]. This process consists of many steps such as identifying, recording, settling, extracting, sorting and reporting exceptions, oddities, irregularities and suspicious transactions, and verifying digital financial data and other accounting activities, with the purpose of making a firm evidence for legal process [2]. Unfortunately, there is no standard procedure to discover all kinds of the frauds yet, as each fraud is a specific case.

So, *forensic accountant* or *fraud investigator* or *fraud examiner* [2, 16, 21] can be defined as an accountant with accounting, auditing and forensic skills that investigates financial fraud case. Sometimes he may be called a *litigation support accountant* and acts as an expert witness on trial in the courtroom [3, 16]. However, if a regular accountant or an accounting auditor wants to become a *forensic accountant* he must take a variety of courses in financial and advanced fraud accounting and auditing, and digital forensic investigation, such as [16, 21]:

- **Digital forensic investigation**: Applied digital forensic principles, procedures, techniques and tools.
- **Forensic accounting:** Applied digital forensic investigation to the accounting.
- **Computers:** Including basic hardware and accounting software (such as *Access, QuickBooks, SAP, Oracle*…).
- **Law:** Basics of business, civil and criminal law, as well as forensic in litigation process.
- **Statistics:** The principles of *chance* or *odds* in the examined transactions.
- **Economics:** Behavioral economics for quantifying damages in litigation.
- **Psychology:** How to handle people, as an advisor?
- **Ethics:** If someone's acts within the limits of the law but is still wrong.
- **Languages:** If a criminal speaks a different language.
- **Criminology:** To understand how the fraudsters work.

To become a *forensic accountant*, someone needs to have forensic accounting; digital forensic and fraud investigation certificates, issued by one of the several professional associations such as *Certified Public Accountant* (CPA) or *Certified Forensic Examiner* (CFE) or *Certified Forensic Financial Analyst* **(**CFFA), etc. [16]. *The Network of Independent Forensic Accountants* (NIFA) is a group of qualified forensic accountants in the USA [2].

Forensic accountants can use some mathematical models, such as *Benford's Law* [1], and *Relative Size Factor* (RSF), as well as *data mining* techniques [5]. The *Benford's Law*, as a duplication program, runs using Microsoft Excel 2007 on Windows XP. *The basis of this law is that fabricated figures (an indicator of fraud) possess a different pattern from random (or valid) figures* [1, 5]. In spite of having a few advantages, the Benford's law has many limitations. The detailed description is done in the article [1]. The *Relative Size Factor* (RSF) detects unusual data that may be caused by errors or frauds [5].

The exponential growth of *big data* and information technology [11], and complex financial transactions and smarter fraudsters pose huge problems to the forensic accounting techniques. However, some advanced techniques such as *data mining* can help forensic accountants [5]. Some of the general characteristics of fraudulent data transactions patterns that can be discovered by specific data mining tools are as follows [5]:

a) Unusual variables or entries of transactions;
b) Unusually high or low value of a variable;
c) Accounting transactions are maintained in various files, and
d) Unexplained values of two or more unrelated records.

3. Integrated Forensic Accounting Investigative Process Model

As the most frauds involve financial matters, the most logical people to investigate them are accountants. However, fraud can be very complex and a digital forensic analyst (DFA) has to be involved in financial fraud investigation process. As financial fraud involves deliberately overstating assets, revenues and profits or understating liabilities, expenses, and losses [2], in such a way that the DFA cannot understand properly, expertise of the professional accountant is inevitable. Otherwise, to avoid the DFA service, the accountants have to be specially trained for digital forensic investigation and analysis. Therefore, employing *forensic*, *accounting* and *auditing* investigative skills into an integrated investigative process model (Figure 1) seems to be very effective in practice.

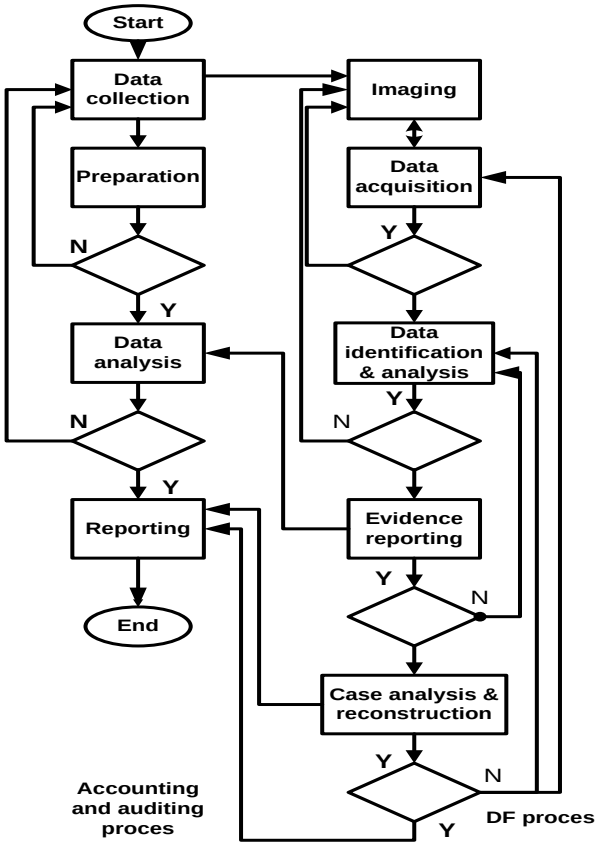

Figure 1: Integrated forensic accounting investigative process model

This process model is in its nature dual processing one. Both accountant and digital forensic analyst (DFA) work together on the same financial fraud case. First, the accountant collects all the available physical and electronic data and information regarding the current fraud case and prepares resources for their analysis. At the beginning of digital forensic investigative process, the DFA takes forensic image of the suspected computer hard disks and/or of financial applications (e.g. MS Excel financial reporting file) and all the other forensically pertinent information. Thereafter, they work separately, but interactively, literally at each decision making point. While the accountant and internal accounting auditor are analyzes all of the collected written and accessible electronic documents, data and information and the other material evidence, the DFA extracts relevant forensic data from the image in acquisition phase, identifying leading data and analyzing them in the next investigative step. After building firm digital evidence regarding the case, the DFA gives over them to the accountant prior to the final reporting phase. Actually, they together reconstruct the case and make the final report to the sponsor (e.g. owner, court or any other stakeholder).

The very first task in the integrated forensic accounting process model is to apply accounting, auditing and digital forensic procedures properly for collection, preservation, acquisition, analysis and reporting physical and digital evidence in the courtroom [9, 19, 21]. When accountant and the DFA together investigate financial fraud, they should go after digital and other physical evidence and look

for the so called *red flags* or *accounting warning signs* or *digital forensic leading data* retrieved from all of the data sources, such as [11, 14]:

- Recognition of revenue before a product is sold;
- Much higher revenues than expenses at the balance;
- Growth in inventory and in sales does not match to each other;
- Expenses capitalization excesses industry norms;
- Reported growing earnings while cash flow is decreasing;
- Much higher growth in revenues comparing to other companies;
- Unusual increases in the book value of assets;
- Impossible to determine the real nature of the transaction;
- Modified or deleted invoices in the financial books;
- Written off loans to the related parties, etc.

In a digital forensic investigative process the following standard forensic operation procedure is crucial to successful and effective computer forensic [7, 15, 18].

1. Protect authenticity of the data sources in imaging phase;
2. Discover and recover all files needed for investigation;
3. Identify and analyze the collected leading data and create the chain of custody, and
4. Summarize findings, make a log of all extracted evidence and preserve their integrity.

In typical financial fraud case, the DFA needs to take forensic image of the accounting computer hard disks (HD), create a hash value of it, and keep one copy as reference and another one as working copy [19, 21]. So, the DFA can parse information from the user's *Recent Docs Registry key*, and the key that listed Excel spreadsheet from the Outlook temporarily file (.pst) and other file server where users could possibly store data in regular backup process. In the next step he/she can extract metadata and see recent modification dates and who has opened or edited or printed the spreadsheet. These metadata includes time stamps correlated to file system and *Registry time stamps*, too [18, 19]. The following forensically relevant data can be saved as hidden information inside a MS Excel documents metadata [4, 15]:

- The names/initials of user, computer and company;
- The name of the server or HD where user saved data;
- Other file properties and summary information;
- Non-visible portions of embedded OLE (*Object Linking and Embedding*) objects;
- The names of previous authors and document revisions;
- Hidden texts and hidden cells;
- Global Unique Identifiers (GUIDs), etc.

Unfortunately, according to the Microsoft's Knowledge Base [17] it is too difficult (if not impossible) to prove when an individual cell or sheet has been modified in a MS Excel file, especially if the *track changes* are not enabled previously. However, forensic accountant or DFA could sometimes be given Excel or another spreadsheet file to be examined. So, document analysis must be involved to find out how many times the file has been "revised", and when the last editing occurred, and the name of the user account that performed the last editing, as well as the last time it was printed, etc. [14, 17].

4. Forensic accounting case investigation and reconstruction

In this financial fraud case, the main accountant from the company "*The last models Ltd*" gave to the DFA two MS Office Excel files, only: One from the ledger at the time of auditing, and the other one from the ledger backup copy file. The integrated forensic accounting investigative model was applied and proved to be effective in this case. The forensic requirements did not include the MS Excel metadata analysis, considering that accounting computer was not accessible. Also, *software forensic* that can be used to identify their authors [6] cannot be easily applied to the MS Excel file, as financial fraud could include change of one number only. Since the company did not have any DFA employed in the security team, its main accountant hired one from the *Association for Information Technology Testimony Witnesses (www.itvestak.com).*

As the first step in the analysis, the DFA checked the size of both files and realized that they were the same. Then he used the open source code forensic tool, *Deft 7.1- Digital evidence and forensic toolkit* [10] to verify file signature, and applied *file comparison* technique. Applying this technique to the sheets with the thousands of entries is very useful, because it reports the differences between the cells on separate sheets. The DFA compared both Excel files without metadata (in *.csv* format), using their MD 5 hash values (Figure 2).

```
[root@localhost Documents]# md5deep orginal.csv manipulacija.csv
37344a380544cf445e89d6ba0a97d6cb  /home/nenad/Documents/orginal.csv
975fbf27420c0463db58796634c600e7  /home/nenad/Documents/manipulacija.csv
```

Figure 2: Files comparison using MD 5 hash values

The hash values proved that those files were not the same, as shown in Figure 2. Checking percentage of the files similarities, using technique of *homogenous files discovery by segmented hashing method initiated with content* [20] (Figure 3), was the next step.

```
[root@localhost Documents]# ssdeep orginal.csv > hash.log
[root@localhost Documents]# ssdeep -bm hash.log manipulacija.csv
manipulacija.csv matches hash.log:/home/nenad/Documents/orginal.csv (99)
```

Figure 3: Homogenous files identification by segmented hashing initiated with content

So, 99% of the two files similarities were identified, suggesting that a small change had been made in one of the two files. The DFA used *Diff* file [10] comparison utility that displayed the differences between the two files, made per line of text files (Figure 4).

```
[root@localhost Documents]# diff orginal.csv manipulacija.csv
5020,5022c5020,5022
<   4817.,05/17/2012,50058,61320        PRIH.OD USLUGA NA INOST TR     ,96,        ,                ,"1,000,000.00",
,,
<   4818.,05/17/2012,50058,20300        POTRAZIV.OD KUPACA U INOST  ,20,        ,"1,000,000.00",                ,                ,
,
<         ,        ,      ,UKUPNO ZA NALOG:                          ,                ,        ,"1,000,000.00","1,000,000.00",
          ,,
---
>   4817.,05/17/2012,50058,61320        PRIH.OD USLUGA NA INOST TR     ,96,        ,                ,"100,000.00",
,,
>   4818.,05/17/2012,50058,20300        POTRAZIV.OD KUPACA U INOST  ,20,        ,"100,000.00",                ,                ,,
>         ,        ,      ,UKUPNO ZA NALOG:                          ,                ,        ,"100,000.00","100,000.00",
          ,,
```

Figure 4: Application of *Diff* utility to find out differences between the two files

Results of the *Diff* tool application are shown in the Figure 4. The two differences no. 5020 and 5022 (red arrows) were identified in the rows of the backup file. The DFA verified the evidence using another forensic tool, *Meld*. This tool has a GUI interface, verifies differences among files and displays retrieved ones. It is slower than *Diff* forensic tool, but it displays results more clearly. As the first step, the *Meld* application starts and a new comparison should be chosen (Figure 5).

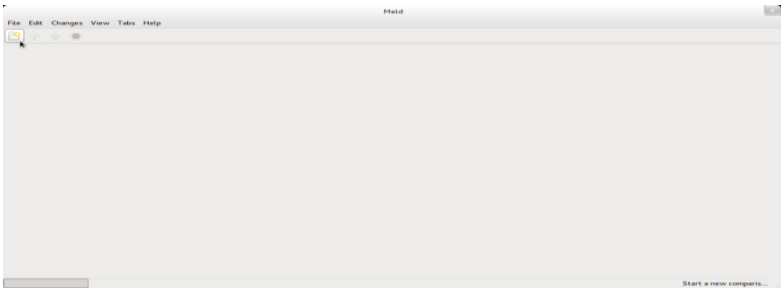

Figure 5: Opening *Meld* tool window

Then, the link to the files that are chosen to be compared should be determined (Figure 6).

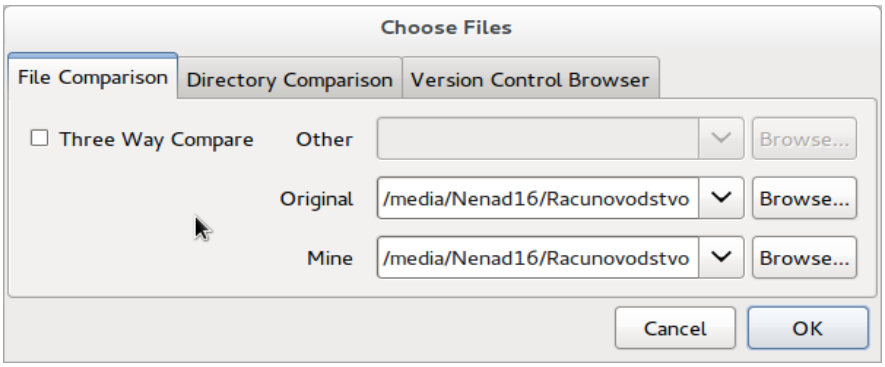

Figure 6: Determination of link to the files chosen to be compared

In the next step the *Meld* tool analyzed and displayed the location where the differences between the two files were found (Figure7).

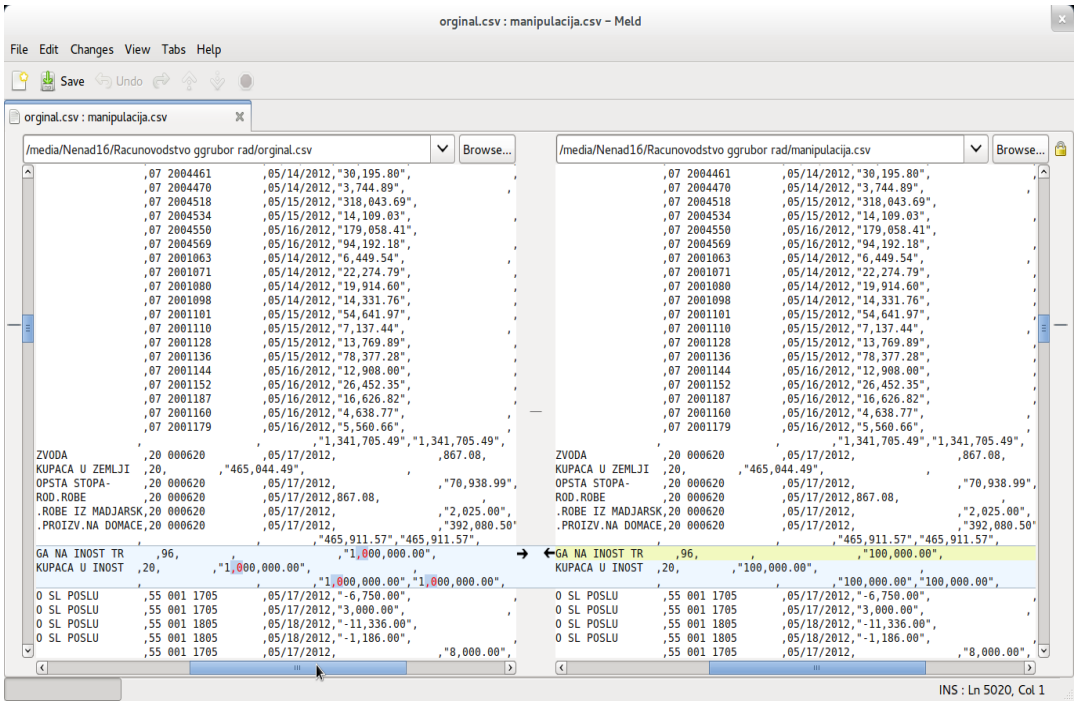

Figure 7: The differences between the two files are highlighted in the *Meld* tool

The *Meld* tool, among other features, indicates location in yellow and detailed differences between these files in red color. However, to satisfy legal request this evidence should be verified with another forensic tool. Verification of the evidence is performed by KDiff3, v. 0.9.96[1]. The KDiff3 is a file and directory *diff* and *merge* tool, comparing and merging two or three text files or directories. It presents the differences line by line and character by character, and provides an automatic merging, too. Having an editor for comfortable solving of merging conflicts, it has options to highlight or hide changes in white-space or comments, and prints differences, as well. Some basic information about the KDiff3 forensic tool is shown in the Figure 8.

[1]Open source code tool, *The KDiff3 Handbook*, www.kdiff3.sourceforge.net.

Figure 8: The KDiff3 forensic tool

As shown in Figure 9 the two changes are displayed and the number of 1,000 000 has been changed with 100 000 one.

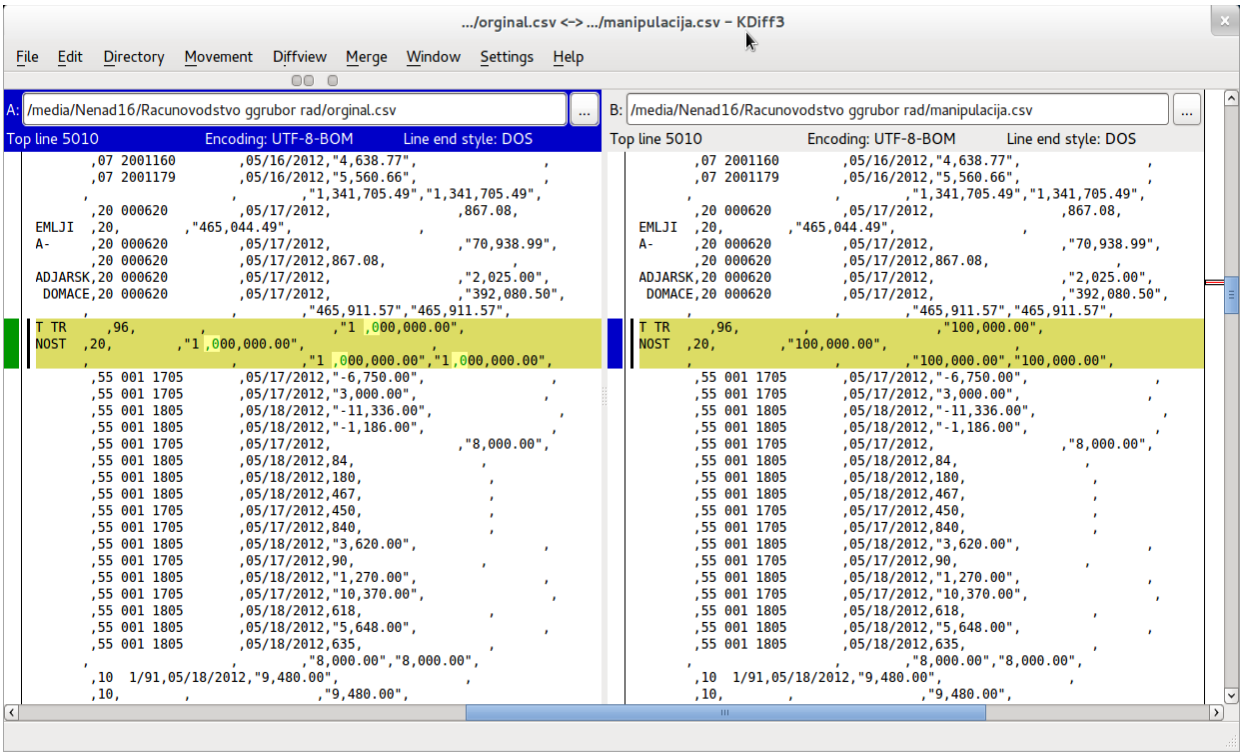

Figure 9: Verification of the files comparison using KDiff3 tool

After verification of the evidence the *KDiff3* forensic tool identified differences at the same place as the *Meld* tool and *Diff* utility did. In this way the verification of the evidence was confirmed twice. So, the main accountant of the company accepted that as a proof of financial fraud.

As it was internal financial fraud investigation case, the main accountant of the company took over the forensic report in order to reconstruct the case together with the DFA. According to the internal audit findings in the company at the end of 2012 year, financial accounting auditor noticed some differences between two financial reports - one reported as a half year balance and another one as the final financial report. Thus, for the first half of the year (2012) the company's recently employed accountant had already made the financial records that were approved by the internal auditor. However, the main accountant became suspicious about some activities of the recently transferred and employed accountant. Therefore, he ordered taking regular scheduled backup of ledger as mandatory activity. In accordance with the company's backup rule - to keep backup files outside of the company, the new accountant copied the ledger in an Excel file format onto his removable hard drive and brought it to his house at the time of the final report. Later on, he changed some data on the backup file and replaced them instead of the already reviewed ledger files. Since these data were approved

at the first half of the year (2012) and the changes decreased greatly debts of the company „F“, the new accountant received some extra money from the debtor. When he bought a new car, manager of the company become suspicious and ordered internal investigation by the main accountant who then hired the DFA, due to the lack of forensic investigation expertise in company.

5. Conclusion

Applying the integrated financial fraud forensic analysis process model, obviously has some advantages in practice, providing forensic accountants and fraud auditors know the financial fraud process very well and the DFA is acquainted with digital forensic science and experienced in different forensic tools and techniques application. They should know how perpetrators commit fraud and the main characteristics of the various fraud schemes. This information can enable them to perform financial fraud investigation effectively or fraud prevention programs. These fraud schemes are a major part of the critical knowledge needed for the accountants, fraud auditors and DFAs to do an effective job. Another major part is the understanding of the red flags associated with these fraud schemes, which are *leading data* for forensic analysis. The DFA has to perform forensic investigation in the way as it will end up in the courtroom. In forensic accounting process the best way is to protect proactively accounting files or logs keeping them centralized and unchanged, than just audit them. They can prove which users accessed, or changed, or deleted or copied some files. File integrity is paramount for every governing regulation and is part of every company's security or digital forensic policy.

In this paper forensic examination of financial fraud is proved by the use of the three forensic tools, *Diff*, *Meld* and *KDiff* and two problems are identified. First, accounting Excel files did not have *Track Changes* activated, and, second, accountant's database server wasn't available to the DFA. This case of the corporate fraud investigation proved that financial accountant, auditor and DFA together can give the best results in financial fraud examination and reconstruction. The DFA followed strict forensic investigative procedure, as the case could eventually end up in the courtroom. Financial accountant and internal auditor performed fraudster's profiling, made fraud scheme and applied forensic analysis results into fraud posture. They reconstructed fraud case together and proved main accountant's suspicious.

For confirmation of benefits of the integrated forensic accounting investigative process model, many more financial fraud cases should be investigated and analyzed in the future. According to the authors opinions, both digital forensic analysis and financial accounting in digital environment are quite complex to be investigated by the same person. Probably, very few people could do quite alone any typical financial fraud investigation in digital environment properly.

Acknowledgment

The authors wish to thank Miss Marijana Prodanović, English language lector of this paper.

REFERENCES

[1] *Benford's Law Excel 2007/2010 software*, Forenzika%20Excela/Benford's%20Law%20Software,%20Excel%20data%20analysis,%20Excel%20forensics.htm,(accessed at 10 of June 2013).

[2] B. K B Kwok, *Forensic Accountancy*, 2nd editions, LexisNexis, 2008.

[3] D. Winch, *Finding and using a forensic accountant*, http://www.accountingevidence. com/documents/articles/Forensic%20accountant1.pdf, October 2007

[4] D. Kernan, *Hidden Data in Electronic Documents*, GIAC GSEC Practical (v.1.4b, Option 1), SANS Institute InfoSec Reading Room, 2004.

[5] Dr. P.K. Panigrahi, *Discovering Fraud in Forensic Accounting Using Data Mining Techniques*, 1426 the Chartered Accountant, April 2006.

[6] E. H. Spafford, Stephen A. Weeber, *Software Forensics: Can We Track Code to its Authors*?, Purdue Technical Report CSD–TR 92–010, SERC Technical Report SERC–TR 110–P, Department of Computer Sciences, 1398 Computer Science Building, Purdue University, West Lafayette, IN 47907–1398, 19 February 1992.

[7] H. Carvey, *Windows Forensic Analysis DVD Toolkit*, Ch. 8, pg. 411, Syngress Publishing. Inc. ISBN 13: 978-1-597-422—9, 2009.

[8] http://www.isaca.org/Journal/Past-Issues/2003/Volume-1/Pages/Using-CAATS-to-Support-IS-Audit.aspx, *Using CAATs to Support IS Audit*(Accessed 20.07.2013).

[9] http://www.fbi.gov/news/stories/2012/march/forensic-accountants_030912/forensic-accountants_030912, *FBI Forensic Accountants*, (accessed at 10 of June 2013).

[10] *http://www.dragonjar.org/deft-digital-evidence-forensic-toolkit.xhtml*, *DEFT (Digital Evidence & Forensic Toolkit)7.01 Manual*, 2013, (Accessed 28.07.2013).

[11] IBM, *Big data at the speed of business*, http://www-01.ibm.com/software/data/bigdata, (accessed at 21, May 2013).

[12] J. Seward, R. Winters, *Forensic Accounting - the recorded electronic data found on Computer Hard Disk Drives, PDAs and numerous other Digital Devices*, LLC NY 10016,JSeward@RWCPAs.com, 2013.

[13] J. R. Jones, *Document Metadata and Computer Forensics*, James Madison University Infosec Tech Report, Department of Computer Science, JMU-INFOSEC-TR-2006-003, 2006.

[14] J. R. King, *Document Production in Litigation: Use an Excel-Based Control Sheet*, National Association of Valuation Analysts, Mar 4, 2009.

[15] J. J. K., Bejtlich, R. Rose, W. C., *Real Digital Forensics - **C**omputer **s**ecurity and **i**ncident **r**esponse*, Addison-Wesley, 2008.

[16] M. Nigrini, *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*, ISBN: 978-0-470-89046-2, Wiley and Sons, 2011.

[17] Microsoft Knowledge Base, *How to minimize metadata in Microsoft Excel workbooks,* Article ID: 223789, Revision: 5.1, 2007.
[18] M. Milosavljević, G. Grubor, *Computer Crime Investigation*, ISBN: 978-86-7912-171-4, University Singidunum, www.singidunum.ac.rs, 2010.
[19] M. Milosavljević, G. Grubor, *Computer System Digital Forensic*, ISBN: 978-86-7912-175-2, University Singidunum, www.singidunum.ac.rs, 2009.
[20] N. Ristić, A. Jevremović, M. Veinović, *Homogenous files identification by segmented hashing initiated with content*, 8. International Telecommunications Forum -TELFOR 2012, ISSN: 20-1665-1668.
[21] T. W. Singleton, A. J. Singleton, *Fraud Auditing and Forensic Accounting*, Fourth Edition, John Wiley & Sons, Inc., 2010.

Authors:
Gojko GRUBOR, PhD, Assistant Professor
ggrubor@sinergija.edu.ba, Department of Informatics and Computing, Sinergija University, Bijeljina, Bosnia&Hetzegovina.
Nenad RISTIĆ
nristic@sinergija.edu.ba, Teaching Assistant, PhD student, Sinergija University, Bijeljina, Bosnia&Hetzegovina, member of the *Association for Information Technology Testimony Witnesses*, Serbia..
Nataša SIMEUNOVIĆ,
nsimeunovic@sinergija.edu.ba, **Teaching Assistant,** PhD student, Sinergija University, Bijeljina, Bosnia&Hetzegovina.

Corresponding author:
Gojko GRUBOR, PhD, Assistant Professor
ggrubor@sinergija.edu.ba, Department of Informatics and Computing, Sinergija University, Bijeljina, Bosnia&Hetzegovina.