Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 01, pp.11700-11707, January, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCHARTICLE

AUTOMATED STRATEGIES FOR COLLABORATIVE INVESTIGATIONS OF DIGITAL LOGS

[1]*Dr Joshua Ojo Nehinbe, [2]Olakunle O Solanke and [3]Johnson Ige Nehibe

[1]UK College of Business and Computing, United Kingdom
[2]Olabisi Onabanjo University, Ago Iwoye, Nigeria
[3]Internal Control Consultant, Nigeria

ARTICLE INFO

Article History:
Received 02nd October, 2014
Received in revised form
15th November, 2014
Accepted 15th December, 2014
Published online 23rd January, 2015

Key words:
Digital Forensics,
Fraudster, Intruder,
Digital Evidence,
Collaborative Investigation,
Miscarriage of justice.

ABSTRACT

Recent advancements in the size, framework, contextual and conceptual understanding of business data across the globe have subjected digital forensics to strict criticisms from numerous angles. Thus, the efficacies of most scientifically proven methods for identifying, collecting, investigating, analysing, interpreting, validating, documenting, reporting and preserving digital evidence rapidly become ineffective to support collaborative digital forensic purposes. Hence, this paper examines some of these core issues and further proposes Log-splitter that can be used to minimize them. In addition, C++ programming language is used to implement the model on the platform of Windows Operating System. The model is subsequently evaluated with series of datasets. The results obtained suggest that Log-splitter can automatically split digital evidence and assigned them to different investigators that are defined by the end-users to quicken the conclusion of digital cases. Furthermore, the results illustrate that investigations of some digital evidence can demonstrate at least three fundamental concepts. Above all, good implementation is the best strategy to mitigate the possibility of biasness of the Log-splitting processes towards one investigator than the other investigators.

1. INTRODUCTION

Series of demands for automated strategies to achieve collaborative investigations of digital logs are increasing globally due to the abrupt changes in the electronic and computer industries in recent years. For instance, the era of standalone computer systems is gradually replaced by series of computer systems that can directly or indirectly interact and exchange data with each other to meet the requirements of end users (Bosworth and Kabay, 2002; Buchanan, 2007; Bishop, 2003 and Kizza, 2009). Unfortunately, these issues enable the size of business data to grow explosively in uncontrollable manner. For some organizations that depend on telecommunication and financial sectors to effectively satisfy their customers, there are possibilities that the data storage capacities they would need can grow up to several gigabytes of information daily, weekly, monthly and annually (Shay, 2004 and Stavroulakis; Stamp, 2010).This trend suggests that such companies may require up to Terabytes data storage space in the nearest future for them for them to strictly adhere to regulatory standards that are required for the length of years that financial data must be kept and secured before they can be legally discarded.

Experience shows that it is usually impractical for some forensic investigators to speedily analyse big digital evidence and subsequently generate needed reports within extremely short deadlines in some peculiar scenarios. Hence, the development of big data is now a central challenge in network forensic analysis of digital logs. This issue can be traced to sudden changes in the size, framework, contextual and conceptual understanding of business data across the globe. Besides, this issue has concurrently created a big challenge to most criminal justice systems in the course of deciding cases involving electronic crimes.

Analyst must construct and reconstruct forensic evidence that will equivalent to eyewitness account of the situation under investigation to establish the case beyond a reasonable doubt. Another possibility is that litigation of suspected electronic criminals can be easily subjected to strict criticisms if a party that has suffered some injury discovers that his or her right to a quick trial is denied by the court of law. Besides, the investigator may not have sufficient automated tools to complete the investigation in all cases whenever he or she is assigned to investigate certain digital logs. Consequently, suspicion, allegations of prejudice and delay of justice may begin to build up. Unfortunately, these issues can easily trigger outcry for legal reforms whereas the underpinning issue is associated with insufficient evidence to conclude the case on time.Another central issue here is that two possible approaches

***Corresponding author: Dr Joshua Ojo Nehinbe**
UK College of Business and Computing, London, United Kingdom.

may be adopted to tackle common or peculiar scenarios that confront forensic investigator in practical investigation of digital logs. The investigator can harness the functionalities in the existing forensic toolkits to extract and report the data (Bradley, 2011; Nehinbe, 2011; Nehinbe, 2012 and Raven *et al*., 2007). Apart from the fact that most forensic tools are proprietary toolkits, investigators mostly require specialized skills to manage forensic toolkits. Another method to tackle the above-named scenarios is to adopt collaborative efforts of multiple experts to investigate digital evidence.

Collaborative digital investigation is defined as the process of engaging two or more digital forensic experts to mutually work as partners with the objective of investigating the same digital crimes. The benefits that characterize collaborative digital investigation of digital logs are many. For instance, collaborative investigation of digital logs can help analysts to achieve accurate analysis of Computer Aided Crimes (CAC) because concerted efforts of experienced professionals with diverse skills are combined together. These procedures can similarly help analysts to avoid or to lessen miscarriage of justice on criminal cases. A miscarriage of justice in a simple term is used to describe a situation whereby people are unjustly convicted, accused or punished for crimes they did not commit. There are many possibilities that can lead to a miscarriage of justice but they are beyond the scope of this paper. In addition, the above processes can help digital analysts to avoid the possibilities of jumping into conclusion due to insufficient analysis of digital evidence.

Importantly, increasing cases of criminals that get away without punishment suggest that most of the scientifically proven methods for digital forensics such as identifying, collecting, investigating and analysing digital evidence are often suggested to strict criticisms. Consequently, this paper proposes Log-splitter to explore the aforementioned four processes and to lessen the issues surrounding them. We extract digital evidence from logs of intrusion detector. Subsequently, we merge some of the extracted evidence together to form big datasets and we later use Log-splitter to evaluate them. One of the contributions of this paper is its potentiality to suggest methods that network forensic analysts can adopt to lessen peculiar problems that are associated with some of the core procedures of digital forensics. Secondly, this paper has suggested methods for generating digital evidence for research purpose. We have also recommended a new method for splitting big digital evidence to support collaborative investigations. The remainders of this paper are organized as follows. Section 2 outlines some of the closely related methods for analysing digital evidence. Section 3 specifies the theoretical concepts about investigation of big forensic data. Section 4 discusses the Log-splitter that is proposed in this paper. Section 5 demonstrates the results obtained from series of evaluations that we conduct with Log-splitter while section 6 concludes the paper.

2. RELATED WORK

There are noticeable trends in the various commercial and research models for analyzing digital logs over the years (Raven *et al*., 2007). In the era of statistical models, probability, correlation and aggregation procedures were proposed to process digital logs (Chatzigiannakis *et al*., 2007; Valdes and Skinner, 2001 and Wenke Lee and Xinzhou Qin, 2003). Some authors have also proposed various forms of clustering techniques to analyze digital logs in the last decades (Bradley, 2011; Nehinbe, 2011 and Nehinbe, 2012).Some of these clustering methods can adopt the values held in the attributes of digital logs while some of them can adopt user-defined variables. The research community has also witnessed another trend whereby some of the earlier models were augmented by combining multiple methods together with the aims to boost prompt detection of digital crimes and the efficacies of the analyses of digital logs. In this era, data mining, genetic algorithm, genetic programming, heuristic and clustering methods were combined with statistical methods to improve accuracy of data analysis (Nehinbe, 2012; Raven *et al*., 2007 and Yan *et al*., 2004). It is imperative to note that some of these methods usually convert low-level (raw) evidence to high level (hyper) evidence using some attributes of digital logs. Similarly, models that have the capabilities to prioritize high level evidence and can equally conduct further tests such as causality test to establish scenarios of attacks in the evidence have been proposed (Yu and Frinke, 2005). Essentially, researchers in this era summarily suggest models for improving the detection rate of digital crimes. Nevertheless, the veracity of such models to achieve high detection rate as well as low false positive rate has generated series of concerns in real work scenarios over the years. If we perceive them in terms of their pragmatic usefulness, adaptability of some of the existing ideas to lessen realistic cases is still questionable. To the best of our knowledge, researchers often shy from designing automated log analyzers that can split digital evidence into suitable fragments and subsequently assign them to cooperative investigators to enhance collaborative analysis across the aforementioned trends.

3. INVESTIGATION OF BIG FORENSIC EVIDENCE

Digital investigation is the process of making a careful inquiry into digital media. Digital experts can convince end users about digital crimes if they have critically studied digital media and gained insightful understanding about digital crimes that they have reviewed. They can achieve these aims by using scientifically certified methods for data analytics and reporting. Unfortunately, the size and sources of digital evidence are increasing in this digital age. As a result, the contextual definitions of digital evidence and understanding of data analytics in general are rapidly developing on a daily basis. The premise here is that in order to thoroughly investigate very big digital evidence in effective and efficient manner, forensic professionals must collaborate with themselves and with service users such as the designers of forensic toolkits to meet the deadline for submitting the reports of their findings to the appropriate authority.

The veracity of these issues can depend on the capability of analysts to split the same digital logs among themselves and in the form that will support collaborative investigation. Capability to achieve this objective will help them to expedite the conclusion of actions necessary to be taken on digital cases that they intend to investigate.

Benefits of automated collaborative investigation of digital evidence

There are gains to engage the services of two or more forensic experts in automated collaborative investigation on the same digital crime. Investigative partners can certainly share professional skills and useful information among themselves without difficulty. They can conduct consistent and well-coordinated investigation within the objective of the examination in a stipulated time. Furthermore, it is possible for the collaborators in this context to discern their individual skills, strengths and weaknesses and such findings can be very useful to strengthen the investigation team and to manage future requirements if there is future need to assemble competent investigators. Additionally, automated collaborative investigations have the tendency to enable the participating investigators to maximize the available resources that are within their disposals to achieve remarkable breakthrough in their quest to establish criminal digital evidence to litigate or to exonerate suspects.

3.1. Issues with automated collaborative investigation of digital evidence

There are potential barriers that can serve as impediments to the motives behind automated collaborative investigation of digital crimes.

3.1.1. Resource intensive

Automated collaborative investigation may be resource intensive. Both physical and nonphysical resources may be expended before laudable progress can be achieved. Besides, it may be difficult to search and secure two or more forensic experts that will be willing to work together and to investigate the same case without wasting ample time that should have been dedicated exclusively to other aspects of digital forensic processes.

3.1.2. Unwillingness to share helpful information

The benefits for automated collaborative investigation may be subverted whenever the participating forensic experts are reluctant to share information among them. In fact, hoarding, subverting and supressing information are detrimental to the success of the team especially if the input to the other investigator is deliberately withheld, delayed or limited by one way or the other.

3.1.3. Generating uniform reports

Generating and agreeing on reports that will be equivalent to eyewitness account are potential barriers to overcome whenever digital forensic experts collaborate to investigate the same digital crimes. Fracas can jeopardize the objectives of the team and in the worst scenarios; some investigators may stubbornly reluctant to accept the opinions suggested by other investigators. Resolving conflicts within the investigators can be time consuming in some cases.

3.1.4. Conflict of interest

Collaborative investigators may have conflict of interest on the same case. They may be reluctant to socialize with each other in a worst scenario. The objectives of this approach may be defeated if they are reluctant to help each other or if they decide to hoard information that will be input to another collaborative colleague to complete his or her tasks.

3.1.5. Disproportionate commitment

There may be disproportionate commitment from the participating investigators especially if they choose to ignore best ethical and professional practices in digital forensics. In essence, lack of agreement in any aspect of the exercise may lead to insufficient intellectual skills and emotional commitment that are expected to sincerely and steadfastly fixity the purpose for pulling resources together to investigate the same digital crime.

3.1.6. Splitting digital evidence

The ultimate goal for splitting big digital evidence is to arrive at distinct subsets. In the example given in Figure 1, the data is split into three subsets of the original evidence. This implies that the three subsets should cumulatively form the parental data whenever they are merged together. Unfortunately, the manner at which digital evidence is related nowadays often makes it possible to have overlapping subsets whenever analysts attempt to split them into smaller components.

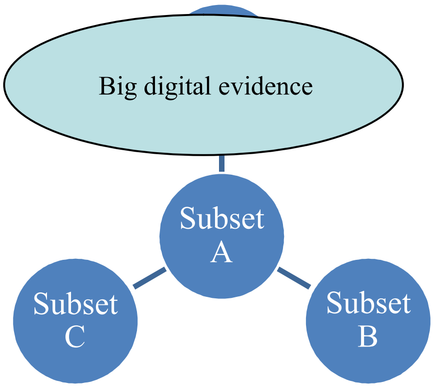

Figure 1. Splitting digital evidence

For instance, it is hardly possible to split massive intrusion logs into two equal and distinct fragments. To lessen this challenge, we can split digital logs such as intrusion logs along the values held for every second of the time to live (ttl) of the alerts. Accordingly, the intrusion logs will form 60 different segments. Thereafter, equal number of segments of the evidence can be automatically assigned to all the designated investigators.

3.2. A method for creating big evaluative digital datasets

We extract digital evidence using the logs of Snort that are generated during offline analysis of Defcon 8, Defcon 10, Defcon 11 and LLDOS 2.0.2 (DA2) datasets (CTFC, 2013; DARPA, 2013). In Table 1, we then generate big datasets by merging them together in varying proportions. Essentially, LLDOS 2.0.2 produced 816 alerts, Defcon 8 produced 909,648 alerts, Defcon 10 produced 4,418 alerts while Defcon 11 produced 8,510 alerts. Total alerts after merging the entire datasets together was 923, 392.

4. THE CONCEPTS OF LOG-SPLITTER

The schematic of Log-splitter that is proposed in this paper is shown in Figure 2. This model is implemented with locally designed computer programs that are written in C++ programming language. The model uses logs as digital evidence, which in turn form the input data to the model. Furthermore, the digital analyzer of the model has two component modules. The first module of the digital analyzer has some inherent rules to split digital evidence. Hence, this model uses such inherent rules to split massive digital evidence into 60 various subsets. The second function of the digital analyzer is to automate common investigative procedures that forensic experts will conventionally adopt to analyze digital evidence. As a result, this component has a default value of 2, which is equivalent to two forensic investigators. So, this component will usually assign at least two forensic investigators A and B to analyze the evidence that has been subdivided into 60 segments. Basically, the numbers of the investigators to be assigned to the fragmented digital evidence are user-defined.

Unlike the common clustering methods for categorizing categorical datasets, this model assigns each forensics investigator to subsets 1 to 30 and subsets 31 to 60 respectively for each of the evaluative datasets used to evaluate our model. It is imperative to note that if the end-users specify any number that is greater than the default value; Log-splitter will require additional information such as the ratio at which the clusters should be assigned to each investigator.

Additionally, an integrator otherwise known as digital integrator accepts input from digital analyzer and harmonizes them into comprehensive reports of all the participating investigators. If the participating investigators are two such as A and B, then, the digital analyzer treats them as InvA and InvB respectively.

Thereafter, it generates holistic digital reports about the evidence. This phase is equivalent to the stage whereby a third forensic expert then merge the reports generated by the two investigators together in a realistic investigation of massive digital evidence. The digital integrator eventually generates the final digital evidence for further usage.

Finally, the above procedures are repeated for every other digital evidence supplied to the Log-filter. The results obtained from the experiments that we conduct are later discussed below.

5. ANALYSIS OF RESULTS

The graphical illustrations of the entire datasets are shown below. Figure 3 shows all the input datasets whenever none of them is split among forensic investigators.

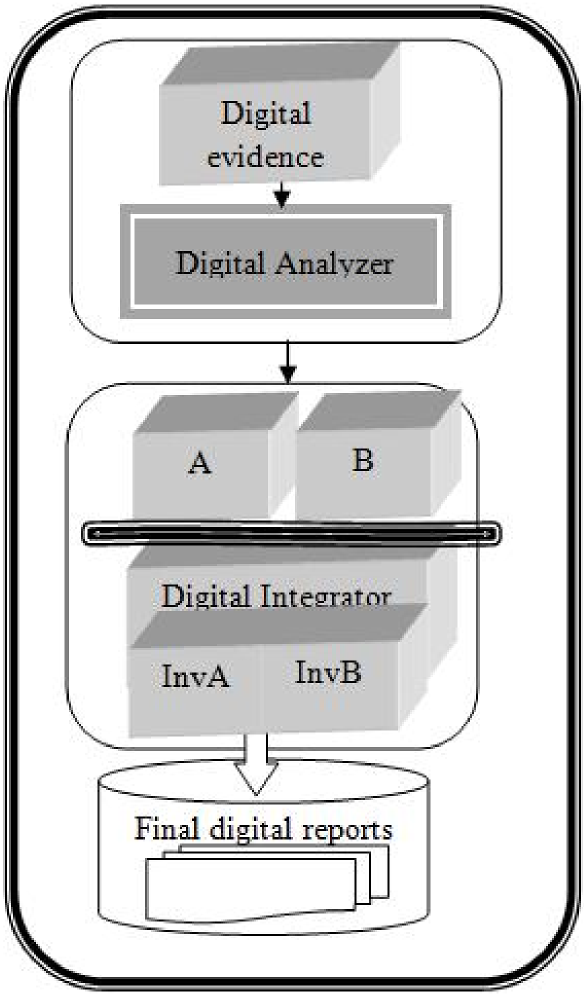

Figure 2. Log-splitter

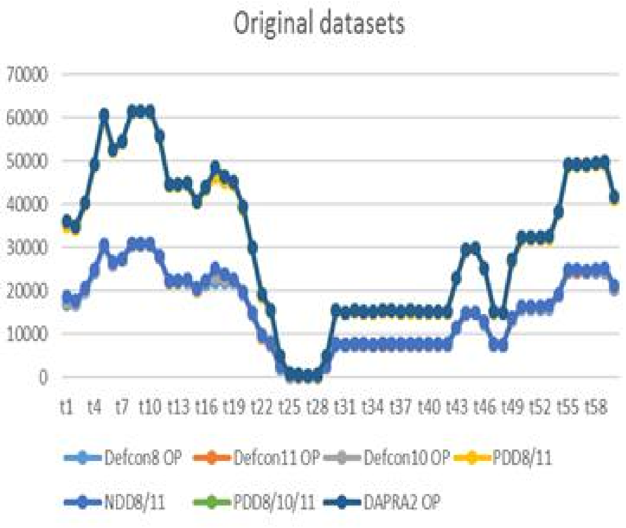

Figure 3. All the datasets

Figures 4 and 5 illustrate the splitting of all the input datasets between two investigators respectively.

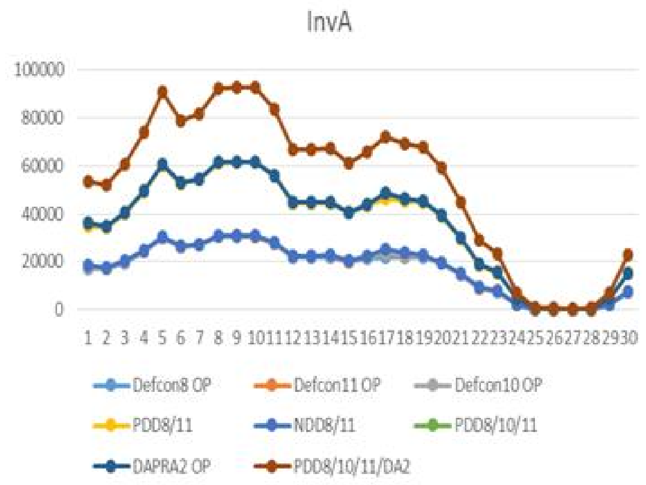

Figure 4. Splitting of all the datasets (InvA)

The results suggest that InvA has less evidence to analyse than InvB between clusters 25 and 28 respectively for most of the evaluative datasets.

According to Figure 5, the contextual meaning of Defcon8 OP, PDD8/10/11/DA2, PDD8/11 and Defcon11 OP are closely related from clusters 1 to 12. The implications of these findings are numerous. The investigator may be able to generate effective reports to describe the events captured within these 12 clusters.

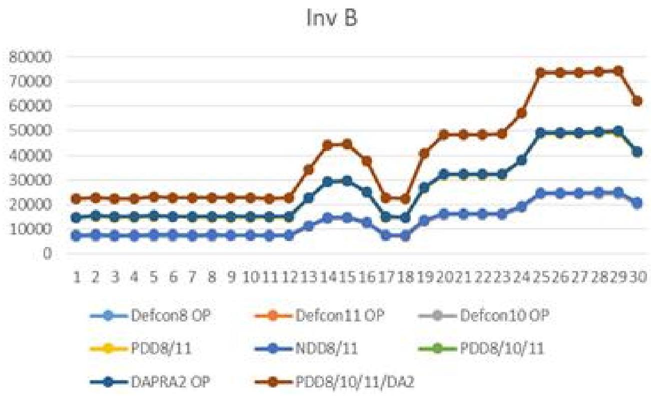

Figure 5. Splitting of all the datasets (InVB)

Furthermore, the collaborative investigators have the reasons to combine their experience and perceptionstogether in other to explicate such findings.

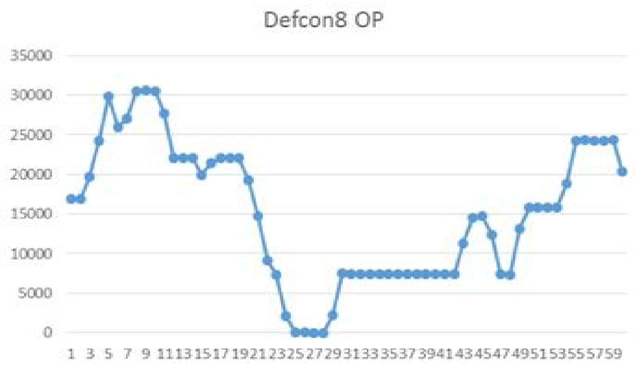

Figure 6. Defcon8 OP (whole data)

Figure 7 shows the whole Defcon11 OP before it is split and assigned to two investigators in Figure 8 and Figure 9. Individual analysis of each dataset has also been investigated.

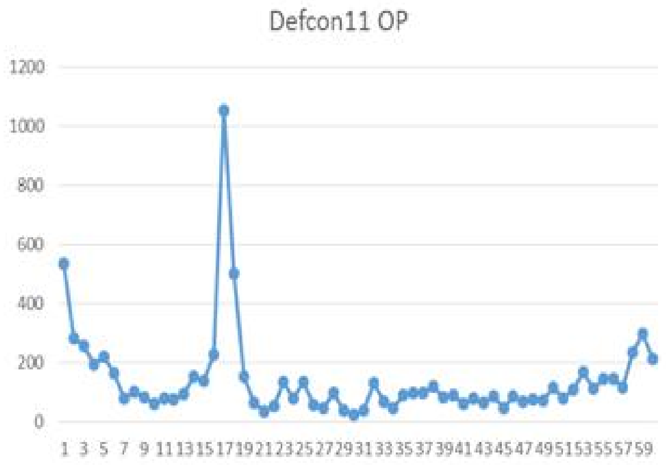

Figure 7. Defcon11 OP (whole data)

Log-splitter suggests that investigator that is assigned to Defcon11 OP (InVA) has more workload when compared to the investigator that is assigned to Defcon11 OP (InVB).

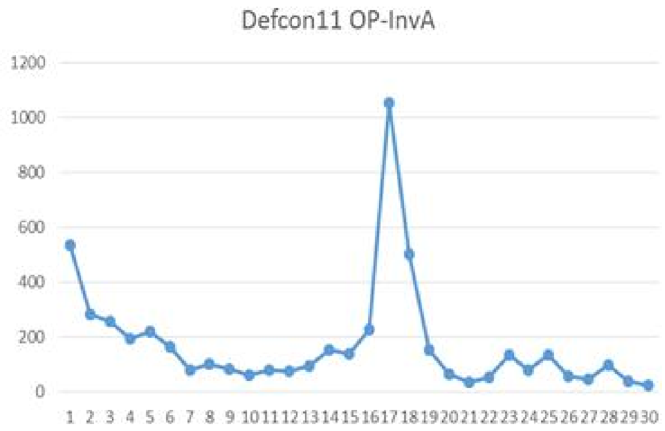

Figure 8. Splitting of Defcon11 OP (InVA)

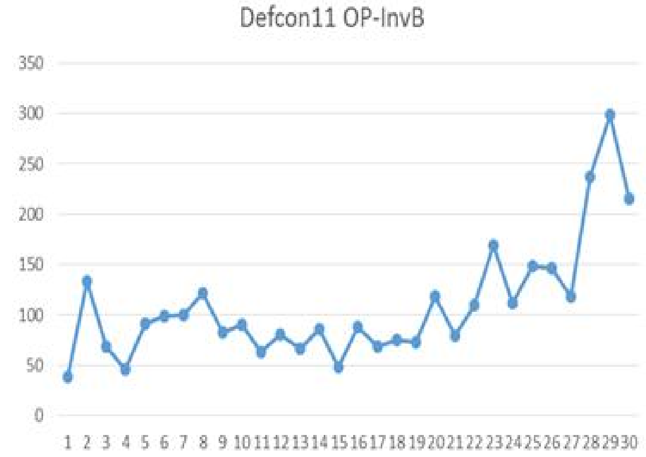

Figure 9. Splitting of Defcon11 OP (InVB)

Figure 10 shows the whole LLDDOS.2.0.2 OP before it is split and assigned to two investigators in Figures 11 and 12 respectively. The results further suggest that the second investigator (InvB) was completely idle while InvA does the entire job.

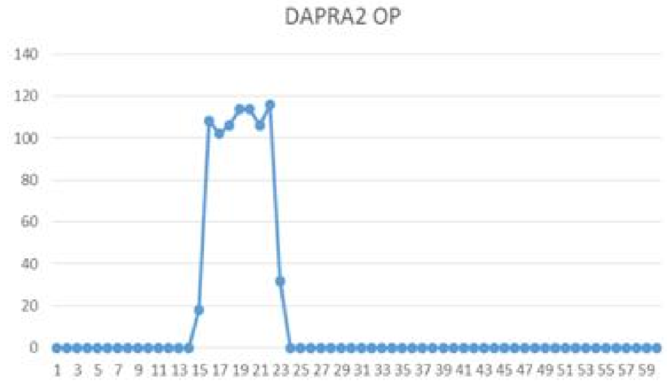

Figure 10. LLDDOS.2.0.2 OP (whole data)

In this case, the splitting of the dataset is skewed towards one side.

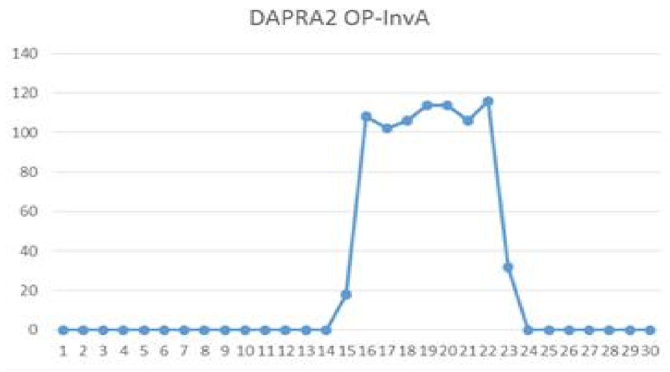

Figure 11. Splitting of LLDDOS.2.0.2 OP (InVA)

Analyses of Defcon 8, Defcon 10 and Defcon 11 datasets suggest that the workload associated with the investigations of available digital evidence in these three sources are biased towards one investigator than the second investigator.

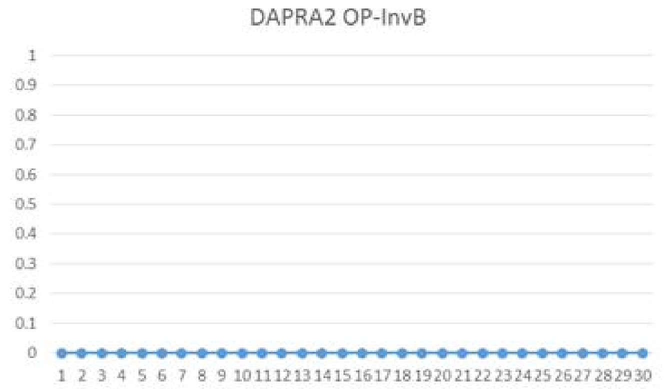

Figure 12. Splitting of LLDDOS.2.0.2 OP (InVB)

In other words, both investigators never shared the same quantity of workload in the course of investigating the above-named three datasets. In other words, Log splitter shows that it is possible for forensic investigators to share closely related quantity of digital evidence as evidenced in Defcon8 OP-InvA and Defcon8 OP-InvB in Figures 13 and 14.

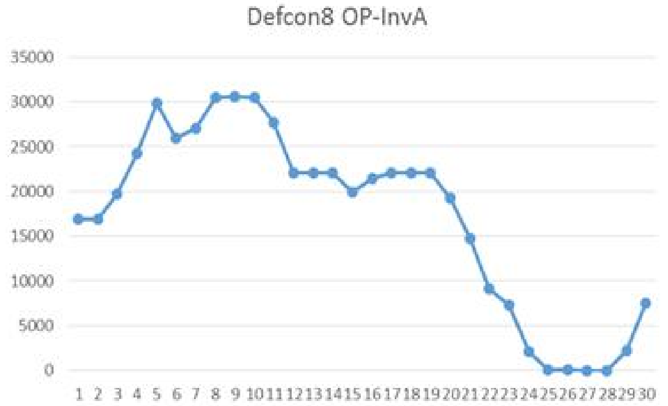

Figure 13. Splitting of Defcon8 OP (InVA)

Essentially, the experimental results above have demonstrated three possibilities during forensic collaborations on the investigations of intrusion logs. Automated collaborative investigation of digital evidence can render some investigators idle. It is also possible that certain investigators are swamped with digital evidence than the other investigators.

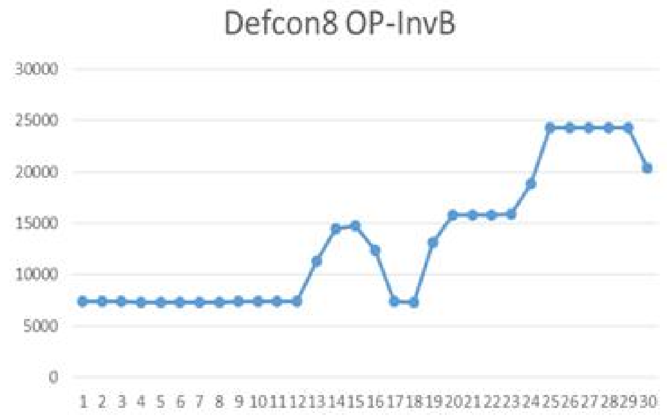

Figure 14. Splitting of Defcon8 OP (InVB)

Finally, the spliting of Defcon8 OP among two investigators suggests that collaborating investigators can be assigned relatively the same quantity of digital evidence.

Table 1. Overview of alerts

Dataset	Alert
PDD8/10/11/DA2	923392
DAPRA2 OP	816
Defcon8 OP	909648
Defcon11 OP	8510
Defcon10 OP	4418
PDD8/11	918158
PDD8/10/11	922576

Table 1 shows the quantity of digital alerts for each dataset. For instance, PDD8/10/11/DA2 dataset indicates sum of alerts from Defcon8 OP, Defcon10 OP, Defcon11 OP and DAPRA2 OP as distributed across the 60 subsets verified above. On the other hand, NDD8/11 indicates negative difference in the quantity of alerts of Defcon8 OP and Defcon11 OP whenever we automatically subtract the content of 60 clusters of Defcon8 OP dataset from corresponding clusters of Defcon11 OP dataset.

Table 2. Overview of variation

Sub-set	Defcon 8 OP	Defcon 11 OP	Defcon 10 OP
t1	16922	535	0
t2	16904	285	0
t3	19696	257	0
t4	24280	194	0
t5	29893	219	0
t6	25994	167	0
t7	27095	79	0
t8	30504	103	0
t9	30640	84	0
t10	30530	60	134

Table 2 shows the variation of the quantity of digital alerts that an investigator would analyse across samples of 3 different datasets.

6. CONCLUSION

Research has recently shifted to the direction whereby crime investigators must ensure that compensation and damages in the form of restitution are not wrongly given to people for unjustifiable claims, loss or injury in attempt to punish electronic fraudsters. This issue is further compounded with the development of sudden changes in the size, framework, contextual and conceptual understanding of business data across the globe. It is a well-established fact that both developments have collectively created a big challenge to most criminal justice systems whenever there is need to establish justice against electronic criminals. Analyst must construct and reconstruct forensic evidence that will equivalent to eyewitness account of the situation under investigation to substantiate the case beyond a reasonable doubt. Another possibility is that litigation of suspected electronic criminals can easily be subjected to strict criticisms if a party that has suffered some injury discovers that his or her right to a quick trial is denied by the court of law. A court may not have sufficient evidence to decide on a digital matter especially if the assigned forensic investigators do not possess sufficient automated tools and professional skills to complete the investigation on time. Therefore, it is plausible to erroneously perceive all or some of the processes to establish the veracity of the incident as prejudice and a delay of justice especially if the issues highlighted above are not correctly managed.

Unfortunately, insufficient evidence to conclude the case on time can aggravate the case. This problem can also subject the investigator to embarrassment and swift opposition from the general public. Fundamentally, digital criminals often search for avenue to clear themselves of accusation, blame, suspicion, or doubt with supporting proofs. Similarly, wrongly accused persons or suspects will also want to vindicate themselves and fight for libel to maintain, uphold or defend smear or character assassination. The paramount goal of lawyers defending a suspect is to acquit their client. On the other hand, the litigating lawyers aim to indict the culprit. These rat races usually generate a though legal battle between the above two opposing parties in quest for supporting evidence. Either party usually leverage on good evidence that are poorly prepared or poorly presented by their contenders. For these reasons, it is imperative to have collaborative efforts for reconstructing forensic evidence so that the involving experts can carefully and thoroughly work together to validate the existing evidence through scientifically certified methods.

Above all, this paper suggests that there are several benefits of working in collaboration to investigate the same digital crime. It has also been suggested that there can be some potential barriers that must be eliminated as impediments to such laudable motive during collaborative investigation of digital logs. Our method has suggested that collaborative investigation can overload some investigators as in the case of LLDOS 2.0.2. In this dataset, the first investigaor (InvA) that analyze subsets 1 to 30 of the datase did all the jobs while the second investigator (InvB) that was assigned to subsets 31 to 60 was completely idle. This observation is a source of open discussion in a realistic situation. Similarly, our model has suggested that collaborative investigation may render some investigators idle. Some investigators may be swamped with digital evidence to analyze while their counterparts may be assigned little evidence to process.

Nonetheless, this paper has not investigated the intrinsic possibilities whenever digital logs are split on the bases of other attributes for a number of reasons. For instance, Log-splitter will skew towards an investigator in the case of computer attacks like Distributed Denial of Service attacks (DDoS) that target only a destination machine if the digital evidence in the dataset is split along the destination address of the attacks. Similarly, further experiments show that it is ineffective to apply Log-splitter to split digital logs using any attribute that will group entire digital evidence into one group. One of the ways to lessen these problems is to enhance our model so that it can adopt the degree of information in the attributes of digital evidence to split digital evidence among respective investigators. Besides, the quality of the research reported in this paper can be improved by focusing on other challenging issues with extremely big digital evidence and their implications to digital forensics. Finally, human beings are essential features of computer security and digital forensics. Hence, researchers still need to focus on automated strategies to model the psyche of potential internal and external threats to corporate data to ensure that the ongoing advancements in the size, framework, contextual and conceptual understanding of business data will not trigger uncontrollable challenges in the nearest future.

REFERENCES

Bradley, W. 2011. A Series of Methods for the systematic reduction of Phishing, PhD thesis, University of Alabama, USA, 2011.

Bosworth, S. and Kabay, M.E 2002. Computer security handbook, fourth edition, John Wiley and Sons, Incorporation, Canada, 2002

Buchanan, W. 2007. The Handbook of Data & Networks Security (1st Edition), Springer-Verlag New York, Inc. Secaucus, NJ, USA.

Bishop, M. 2003. Computer Security: Art and Science, Pearson Education, Inc, New York

Chatzigiannakis, V., Androulidakis, G., Pelechrinis, K., Papavassiliou, S. and Maglaris, V.2007 Data fusion algorithms for network anomaly detection: classification and evaluation, Network Management & Optimal Design Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens.

Capture the flag contest (CTFC) (CTFC, 2013). Defcon datasets http://cctf.shmoo.com/ data/Accessed 12 May April 2013

DARPA, 2013. Intrusion Detection Scenario Specific Datasetshttp://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000data.html; Accessed 28/08/2013

Kizza, J.M. 2009. A Guide to Computer Network Security, Springer-Verlag London, 2009

Nehinbe J.O. 2011. Methods for reducing workload during investigations of Intrusion Logs, PhD thesis, University of Essex, UK, 2011

Nehinbe J.O. 2012. A comparative study of attributes for gathering admissible evidence in the investigation of Distributed Denial of Service (DDoS) attacks, IJITST, Vol. 4, 2012

Raven, A., Baker, R.B., Carter, J.F., Esler, J., Foster, C.F., Jonkman, M., Keefer, C., Marty, R. and Seagren, E.S. 2007. Snort: IDS and IPS Toolkit, Syngress publishing, Burlington, Canada.

Shay, W.A. 2004. Understanding Communications and Networks, Brooks/Cole, USA

Stavroulakis, P. and M. Stamp. 2010. Handbook of Information and Communication Security, Springer-Heidelberg,New York, 2010.

Valdes, A., and Skinner, K. 2001. Probabilistic alert correlation, in proceed of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001), October, 2001.

Valdes, A., and Skinner, K. 2000. Adaptive, Model-Based Monitoring for Cyber Attack Detection, in proceedings of the 3rdInternational Workshop on Recent Advances in Intrusion Detection, pages 80-92, October, 2000

Wenke Lee and Xinzhou Qin, 2003. Statistical Causality Analysis of INFOSEC Alert Data, RAID, Springer Verlag, pages 73- 93, 2003.

Yu, D. and Frinke, D. 2005. Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory, Department of Computer Science, University of Idaho.

Yan, Z., Peng, N., Purush, I. and Reeves, D.S. 2004. Reasoning about Complementary Intrusion Evidence, Cyber Defense Laboratory, Department of Computer Science, North Carolina State University, Raleigh, NC 29695-8207

****