A Method for Reducing the Risk of Errors in Digital Forensic Investigations

Graeme Horsman, Christopher Laing, Paul Vickers

A Method for Reducing the Risk of Errors in Digital Forensic Investigations

Graeme Horsman, Christopher Laing, Paul Vickers

Computing, Engineering and Information Sciences
Northumbria University, Newcastle-Upon-Tyne, United Kingdom
Graeme.horsman@springer.com

Abstract. Motivated by the concerns expressed by many academics over difficulties facing the digital forensic field, user-contributory case-based reasoning (UCCBR); a method for auditing digital forensic investigations is presented. This auditing methodology is not designed to replace a digital forensic practitioner but to aid their investigation process, acting as a method for reducing the risks of missed or misinterpreted evidence. The structure and functionality of UCCBR is discussed and its potential for implementation within a digital forensic environment.

Key Terms: Digital forensics; Auditing; Case-based reasoning; Contributory

1. Introduction

Bem [1] speaks of an impending crisis for the field of digital forensics (DF), an opinion shared by other academics [3][6][7]. The speed of technological development [13], increasing digital storage media capacities [14] and growing cyber crime figures [10] are all reasons cited as contributing factors. DF practitioners are facing added pressures from the demands placed upon their already stretched resources, where case backlogs have already been identified in High Tech Crime Units across the United Kingdom [8]. In an attempt to combat these demands research has focused on the development of frameworks, which attempt to increase the efficiency of DF investigations. The Cyber Forensic Field Triage Process Model (CFFTPM) developed by Rogers *et al* tries to address the issue by preforming the onsite triage of data [2]. Freiling's [4] model is developed for incident response as a systematic approach to reacting to unauthorised actions or breaches. Automated processes have been theorised in an attempt to replace the DF practitioner and assist in the management of their workload [5]. The overarching issue with these approaches is that they attempt to revise the way in which current DF investigative practices operate. One of the major drawbacks to this is that it requires the adherence of the field of DF and their practitioners to adopt such strategies. This in turn requires the standardisation of DF practices and principles, an area, which the field currently lacks [1][11]. This paper argues that focus should be on developing methods for ensuring practitioner investigation standards are maintained as they become subjected to greater pressures.

2. Motivation

This research has developed from a need for strategies to reduce the risks of any mistakes made by DF practitioners. The authors agree that the development of tools capable of automating the DF investigation process is a future goal for the field, but such techniques are currently in a stage of infancy and not capable of providing the levels of investigative support that have been identified as necessary [9]. Instead, the authors argue that attention should be placed on the development of methods for auditing and evaluating DF investigation results in an attempt to limit the risk of errors occurring. This has lead to the development of user-contributory case-based reasoning (UCCBR) as a method for auditing DF investigation results.

Digital evidence is becoming a more prominent factor in many criminal investigations due to the increase of cyber crime [10]. This in turn directly impacts upon the workloads of DF practitioners arguably subjecting them to more stress as they attempt to cope with increased workloads whilst adhering to strict timeframes. It has been identified in other forensic disciplines that subjecting practitioners to similar increased levels of stress has a negative impact upon the quality of the work they produce [11]. Therefore it is necessary for the field of DF to take steps towards the development of investigation auditing to ensure that the quality of investigations is maintained. It is commonly recognised that DF software should be validated to ensure that a satisfactory outcome is produced by its operation [12], yet little consideration is given to the actual user of such tools. Both Sheldon [13] and Brushi [14] are concerned that due to the complexity of DF investigations, it is no longer possible to rely on the accuracy of any one practitioner's results. As an auditing system, UCCBR becomes a safety net for the examiner highlighting the potential of an erroneous investigation before it is too late for a DF practitioner to correct.

3. Auditing Digital Forensic Investigations

Auditing is used to assess existing criterion against a known satisfactory set of principles [15]. The goal of such a process is to highlight any weaknesses which may exist and then propose methods for improvement. In the realms of DF, an investigation audit is designed to evaluate the results obtained from a DF investigation by a practitioner. It can provide a method of limiting the risks of unfinished investigations. Many DF organisations rely upon the competency and ability of their practitioners to produce casework to a high standard, typically to a level where evidence is permissible in a court of law. Yet very few organisations directly evaluate the quality of any DF investigation undertaken by their staff. Peer review is a usual technique adopted where colleagues attempt to address any issues that may be inherently obvious due to the investigation type. However, this strategy may fail to identify any underlying issues, which have occurred during an investigation such as missed, or misinterpreted data. A DF peer review rarely offers a comprehensive evaluation of the work that has been undertaken which could be generated through an auditing process.

Unaudited DF examinations provide a number of risks to a DF organisation and its practitioners. First it becomes difficult to determine whether an investigation is complete and all evidence that exists has been collected and reported by a practitioner. Second, practitioner error may remain undetected leaving and results vulnerable to dispute in a court of law. As part of a DF organisations risk management strategy, it should be seen as a necessary step to ensure procedures are in place to safeguard their standard of their DF investigations, one of the main services they offer.

In order to audit DF investigations a level of knowledge and experience of the topic area is needed. This could involve a second examiner reinvestigating the case in which the primary examiner has already completed in order to confirm or deny the results provided by the primary examiner. This method is impractical and most DF organisations will see this behavior and an inefficient use of resources, however, the underlying principle has some merit. A second review of an investigation subjects it to the experience and knowledge of another, which can prove valuable given the concept that there is potential for a greater amount of knowledge and experience to be present with two or more practitioners rather than one. A successful audit system would have to encapsulate the knowledge and experience of fellow practitioners in order to evaluate the results of a DF investigation [28].

UCCBR is a system that incorporates knowledge from multiple DF practitioners in order to evaluate the results of a DF investigation. DF investigations of the same offence type may share similar evidential traits. For example, an offence of fraud may display characteristics which are comparable to other investigations of fraud. UCCBR can utilise these similarities when used to audit a future DF case. Where such data was known to contribute towards identifying a previous offence, it becomes relevant for use when auditing a future case. Where a future case shares partial similarities to an offence of fraud, as used in this example, UCCBR can suggest its previous investigative experience of fraud as a means to evaluate the content of the present examination under audit.

An objective of a UCCBR system is to facilitate knowledge sharing in DF investigations and is dependent on the submission of knowledge by DF professionals. UCCBR is aimed at a single organisation where multiple DF practitioners are employed. Each practitioner would contribute the results of their investigations to the system. Practitioners within the organisation would have access to the UCCBR system and in turn the knowledge contributed by fellow peers. A UCCBR system would provide a valuable risk assessment during an audit, as it would contain knowledge of areas and files known to contain relevant data in previous investigations.

4. UCCBR Explained

The authors are currently developing UCCBR [28] which is a novel version of a conventional case-based reasoning (CBR) methodology. CBR systems are widely used and have been successfully implemented in many professional fields [19] [20]. CBR is predominantly a method for problem solving which is achieved by reusing documented solutions to previously similar problems [21]. CBR systems have a storage area which is used to accumulate cases, which are then retrieved and used as part of the system's overall function of problem solving. The case base stores the systems experience which is needed for the system to accurately and successfully problem solve. As the number of cases in the case base increase, so does the systems experience, increasing the probability of the solutions that the system produces will be correct [20].

There are four main stages to a CBR system [21] [22]. The first is to identify the scope of the problem which is in need of solving. Second, the CBR system must identify a case from its case base which can offer the best solution to the problem that is being addressed [17]. Third, the case containing the solution must then be retrieved and used as part of the problem solving process. Finally the selected case must then be reviewed to ensure that the solution it contains is the most appropriate and if a better solution exists the case is then revised to accommodate this [28].

UCCBR is a system built upon the principles of current CBR structures but adapted to allow the case base to be constructed through multiple submissions acquired from DF practitioners. Each submission to UCCBR from a practitioner is submitted as a case into UCCBR's case base and consists of the results from their past DF investigation. The case base for UCCBR is an area used to stockpile cases which have been submitted to the system by practitioners. Each case contains the results of a previous DF investigation which have been previously undertaken by a DF practitioner. Each case will contain details of a particular offence, showing how the offence was committed in that particular occasion. Each case will document the details of relevant files that the primary examiner in that investigation has found during the examination, which in turn will be used in future investigations to identify similar activity[28].

Case bases for traditional CBR systems are often built by an expert who makes sure that only correct and accurate data enters the system. To avoid such errors often the number of experts who have access to a case base will be limited. This is often seen as an attempt to reduce the risk of human error. The disadvantage to this approach is that often there is an increase in the time needed for a CBR system to amass a case base with a large number of cases. In a UCCBR system, a case base is created through contributions from multiple practitioners acting as experts for the system. The case base is constructed using data from real events documented in actual DF investigations and obtained from multiple DF practitioners. Given the notion that there is a greater potential for knowledge from ten experts than one, a contributory method for case base construction has the potential to create a more competent case base [20].

The case base provides the system with past experience of problems, which is needed for problem solving. The more cases stored in the case base the more experienced the system becomes giving the overall system a higher potential for accuracy in the solutions it produces [20]. The value of the case base increases with the amount of cases that are entered [21].

A UCCBR system also circumvents any chances of the case base being subjected to any prejudice as its population is not subject to a single or limited number of experts. In this circumstance, a single expert may be tempted to populate their system with knowledge, which is known to make it produce favourable results in artificial testing scenarios. However, this may not necessarily reflect accurate results when faced with solving real problems. As UCCBR takes results from multiple sources in actual investigatory scenarios, its case base consists of a more accurate depiction of the suspect offences. Restricting the creation of a case base to a single or limited number of experts comes with its own risks. The case base then becomes subject to any gaps in knowledge that such experts have and therefore lacks solutions, which could be offered by experts further afield. A UCCBR case base is generated from a far wider source of data encapsulating the knowledge and skill of many practitioners.

5. How UCCBR Functions

UCCBR maintains a number of case bases which are separated into different offence types (see Fig. 1.). This allows UCCBR to target the audit at a specific offence as different offences maintain different characteristics. When a practitioner submits a case to UCCBR it becomes a sub case in relation to the offence that particular practitioner has undertaken. In fig.1 sub cases one, two and three are all fraud based examinations. UCCBR then generates a fraud primary case, encapsulating the knowledge from all fraud sub cases. If a fraud case is submitted for audit UCCBR selects the appropriate primary case in relation to the offence of the investigation due for auditing and derives its audit from the investigative knowledge stored in this area of the case base.

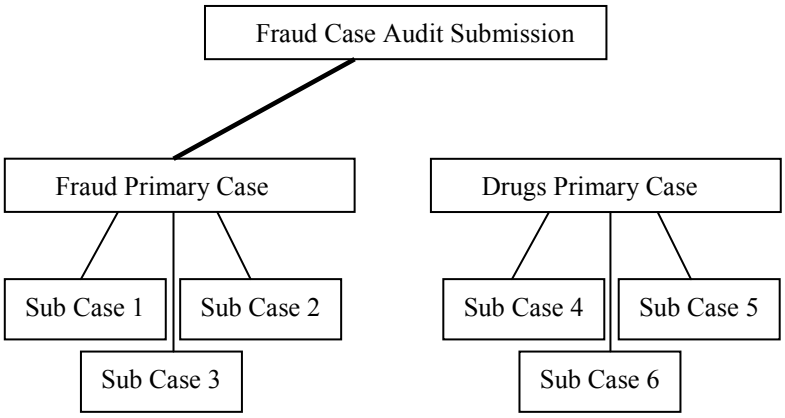

Fig.1. Structure of UCCBR case base

UCCBR does not function in the same way as traditional CBR in that it does not produce a solution from one particular case. As DF investigations have a potentially unlimited number of characteristics, it is necessary to consider aspects from all cases stored in the case base relating to that offence. Where similarities and partial matches occur between the case for audit and any sub cases in UCCBR, a comparison is made. Fig.2. demonstrates the way in which a comparison is made during an audit by UCCBR. When an investigation is submitted for audit, it contains the locations of evidence found by the practitioner. UCCBR uses the audit case and looks for similarities in its case base which are shared with previous cases of that particular offence type. In the example in Fig.2 the audit produces a match on items A and B. UCCBR identifies a case which has matched items A and B and has knowledge of evidence at items C and E which had been found in this particular case. These items are not present in the investigation under audit but have previously been found in past DF investigations. In this example items C and E are suggested as the potential areas of concern for the DF investigator and must be verified as the case for audit shares similar characteristics to this case.

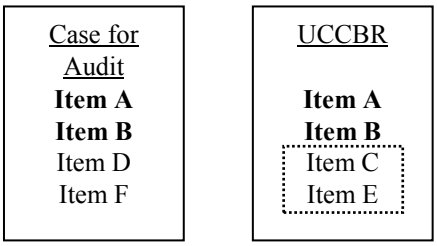

Fig.2. Audit Example

UCCBR can provide a practitioner with reassurance that they have carried out a correct investigation by validating their results against what is classed as commonly seen activity for a given offence. This validation may confirm what an examiner has already done in terms of the investigation and that the types of evidence they have found is consistent for that offence type. Additionally, it may inform an examiner of further areas to investigate where relevant data has been known to reside as in the example given in Fig.2. UCCBR maintains the added advantage of a case base that contains actual investigation knowledge gathered from practitioners in the DF field. UCCBR can surpass the standards of evaluation achieved by simple peer reviews and provides an important level security for both the practitioner and a DF organisation when attempting to reduce the risk of errors in DF investigations.

As UCCBR contains a large quantity of knowledge used for decision making and can offer a number of advantages over a single practitioner's ability to audit and identify risks in a DF investigation [24]. A single examiner is limited to the knowledge that they can remember and evoke during an audit [25]. Due to the complexity of DF investigations it is unlikely that they would be able to form accurate auditing decisions formed from their potentially limited knowledge [26]. This is where a UCCBR system

can benefit the field of DF is has the ability to hold a potentially infinite amount of data which can be utilized during an audit. A UCCBR system that has accumulated accurate knowledge from a number of external sources possesses the ability to house and apply a greater amount of knowledge than any one DF practitioner.

6. Conclusion and Future Work

This paper has proposed a UCCBR DF investigation audit system designed to evaluate DF investigations in an attempt to limit the risk of errors. As the field of DF is directly impacted by the increase of cyber crime it is necessary to implement auditing to ensure investigation standards are sufficient. An auditing system provides a fail safe for the DF practitioner by identifying the risk of overlooked or misinterpreted data before an examination is deemed to be complete. A prototype UCCBR system is being developed for use in auditing DF examination results, which will be tested within a small DF organisation. Additionally, further work is being carried out with regards to the reasoning algorithms that have been implemented for forming the auditing decisions made by UCCBR.

References

1. Bem, Derek; Feld, Francine; Huebner, Ewa; Bem; Oscar, 'Computer Forensics - Past, Present and Future', Journal of Information Science and Technology, 2008 5(3) 43-59
2. Rogers, M. K., Goldman, J., Mislan, R., Wedge, T , & Debrota, S. 'Computer Forensics Field Triage Process Model, Conference on Digital Forensics, Security and Law' 2006 from http://www.digitalforensics-conference.org/CFFTPI\/l/CDFSL-proceedings2006-CFFTPM.pdf.
3. Lalla, Himal; Flowerday, Stephen V. 'Towards a Standardised Digital Forensic Process: Email Forensics' 2010 Information Security for South Africa (ISSA 2010) Conference
4. Freiling, F. C.; Schwittay, B. 'A Common Process Model for Incident Response and Computer Forensics' 2007 Proceedings of Conference on IT Incident Management and IT Forensics. Germany.
5. Richard, G.G.; Roussev. V. 'Next-generation digital forensics' 2006 Communications of the ACM, 49(2):76–80,
6. Sheldon, A. 'The future of forensic computing' Digital Investigation, 2005, 2, 31-35
7. Bruschi, D. & Monga, M. 'How to Reuse Knowledge About Forensic Investigations' Digital Forensics Research Workshop, 2004
8. ADF, 'Triage Solutions for Evidence and Intelligence Acquisition' 2010 Accessed: 24th March 2011
9. Ayers, D. 'A second generation computer forensic analysis system' Digital Investigation, 2009, 34-42, 6
10. Taylor, Carol; Endicott-Popovskyb, Barbara; Frinckec; Deborah A. 'Specifying digital forensics: A forensics policy approach' Digital Investigation, 2007 101–104, 4
11. National Institute of Standards and Technology, 2012 ''Expert Working Group on Human Factors in Latent Print Analysis. Latent Print Examination and Human Factors: Improving the Practice through a Systems Approach.' U.S. Department of Commerce
12. Erbacher, Robert F. 'Validation for Digital Forensics' 2010 Information Technology: New Generations (ITNG), 2010 Seventh International Conference on

13. Bruschi, D. & Monga, M. ‘How to Reuse Knowledge About Forensic Investigations’ Digital Forensics Research Workshop, 2004
14. Sheldon, A. ‘The future of forensic computing’ Digital Investigation, 2005, 2, 31-35
15. Jamil, S.; Aeiker, J. D. & Crow, D. R. ‘Auditing is Key’ IEEE Industry Applications Magazine, 2010, 16, 47-56
16. Aamodt, A. & Plaza, E. ‘Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches’ AI Communications, 1994, 7, 39-59
17. Xu, L. ‘Developing a case-based knowledge system for AIDS prevention’ Expert Systems, 1994, 11, 237–244
18. Guidance Software ‘EnCase Forensic’ 2012 Available at: http://www.guidancesoftware.com/forensic.htm
19. Rissland, E.; Kevin, A. & Branting, L. K. ‘Case-based reasoning and law’ *The Knowledge* Engineering Review, 2005, 20, 293-298
20. Katedee, S.; Sanrach, C. & Thesawadwong, T. ‘Case-Based Reasoning System for Histopathology Diagnosis’ *Educational and Information Technology (ICEIT), 2010 International Conference on,* 2010
21. Kolodner, J. ‘An Introduction to Case-Based Reasoning’ *Artificial Intelligence Review,* 1992*, 6*, 3-34
22. Kerr, S. G.; Jooste, S.; Grupe, F. H. & Vreeland, J. M. ‘A case-based approach to the evaluation of new audit clients’ *Journal of Computer Information Systems,* 2007*, 47:4*, 1927
23. Aamodt, A. & Plaza, E. ‘Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches’ *AI Communications,* 1994*, 7*, 39-59
24. Keppens, J. & Schaferb, B. ‘Knowledge based crime scenario modelling’ *Expert Systems with Applications,* **2006***, 30*, 203–222
25. Dudai, Y. ‘How Big Is Human Memory, or On Being Just Useful Enough’ *Learning and Memory* **1997** 3, 5: 341–365.
26. Timmermans, D. ‘The Impact of Task Complexity on Information Use in Multi-attribute Decision Making’ *Journal of Behavioral Decision Making* **1993** *6, 95-111*
27. Reeson, A and Dunstall, S. ‘Behavioural Economics and Complex Decision-Making; Implications for the Australian Tax and Transfer System’ **2009** Available at: http://taxreview.treasury.gov.au/content/html/commissioned_work/downloads/CSIRO_AFTS_Behavioural_e conomics_paper.pdf (Accessed 1st February 2012)
28. Horsman, G and Laing, C. and Vickers, P ‘A Case Based Reasoning Framework for Improving the Trustworthiness of Digital Forensic Investigations’ The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012