IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 5, Issue 2, February 2017 ISSN 2321-5992

An Approach for Managing Knowledge in Digital Forensic Examinations

Miss. Selpi Chouhan

University College of Technology, Osmania University, Hyderabad

ABSTRACT

Cancelable biometric techniques are becoming popular as they provide the advantages of privacy and security, not provided by biometric authentication system. It transforms a biometric signal or feature into a new signal or feature by some transformation. These are non invertible transforms to make sure that the original biometric template cannot be recovered from them. Most of the existing methods for generating cancelable fingerprint templates need an absolute registration of the image. Therefore they are not robust to intra user variations. But there also exists methods that do not require registration of the image. This paper provides a comparison between two such methods, one that needs registration and other that does not need registration.

1. INTRODUCTION

of the various problems related to pc forensics, information management methods also are necessary to the longer term of not solely pc forensics, however digital forensics yet. many models are developed. These models square measure extensions of the DFRWS model that served because the basis for digital rhetorical modeling approaches. These models centered on the investigatory method and also the totally different phases, they addressed the complexness of associate investigation and also the options and practicality of devices, and also the concrete principles of associate investigation. Of the models listed, one centered on a selected part and created empirical results. Empirical results of actual application and usage of modeling approaches by digital rhetorical investigators square measure lacking considerably. analysis involving investigators is very restricted in digital rhetorical analysis, particularly once specializing in the examination part of a digital rhetorical investigation. Reasons for this could be that investigators can't perceive the modeling approach, investigators is also hesitant to be told a brand new methodology or model and should suppose their own division or structure procedures, and/or investigators is also unaware of the various modeling approaches. In either of the cases, analysis is lacking to see if, in fact, modeling approaches square measure being employed in the slightest degree in digital investigations. moreover, analysis is additionally required to handle information management methods in pc forensics. per [18], “Effective information management maintains the information assests of a company by distinguishing and capturing helpful data in a very usable kind, and by supporting refinement and apply of that data in commission of the organization’s goals. a very necessary quality is that the internal information embodied within the expertise of task consultants which will be lost with shifts in comes and personnel.” there's a necessity for information management in digital forensics attributable to the enhanced usage of the net, the rise in digital crimes victimization differing kinds of digital media, and also the constant advances in technology. A simplified methodology for capturing and reusing digital crime information may sway be valuable to the enforcement community. silent information or knowledgeable information is largely an indoor knowing of what must be done and the way it ought to be done [18]. pc crimes square measure increasing, and there's an excellent would like for information sharing amongst the native, state, and federal authorities to additional combat these crimes. once pc rhetorical examiners perform examinations, their specialised skills might not be recorded. These specialised skills can be terribly helpful for external reviews and coaching. skilled and full-fledged personnel apprehend what to appear for, wherever to appear, and the way to appear while not compromising the proof. Externalizing this information may assist novice examiners in investigations and will doubtless result in the creation of a knowledge repository. In most cases, digital rhetorical examiners should search through giant amounts of information to search out proof. With digital storage capacities changing into progressively larger, this task is changing into even additional complicated and time intense. information management methodologies within the pc forensics domain are addressed in [19] [20]. Bruschi, Monga, and Martignoni [19] planned a model that organizes rhetorical information in a very reusable manner. This model uses past experiences to coach new personnel, to alter information sharing among detective communities, and to permit third parties to assess the standard of collected data. They additionally steered that disciplined methodologies ought to be created that give the chance of archiving digital rhetorical information that may aid in coaching and best apply tips. a way for effectively reusing and managing information may greatly improve the digital rhetorical method. per [20], the apply of digital forensics can be increased by developing “knowledge management methods specific to enforcement that may operate inside the particular

context of criminal investigations". In [19], their approach aims to produce a "methodology for archiving, retrieving, and reasoning concerning rhetorical information, so as to incrementally improve the abilities and also the work of a team of detectives." Their planned software package tool and approach can turn out reusable rhetorical information as support throughout investigations, can organize past expertise to encourage information sharing among rhetorical consultants, and can record collected data in a very manner that eases quality assessment. so as to demonstrate the importance of capturing and reusing information, Kramer utilised idea maps to produce a way for capturing the silent information of style method consultants. Kramer's [21] research tried to gather, understand, and apply the information of multiple domain consultants on style processes that drive initial style choices related to translating "Requirements on Orbit" to "Design needs." idea maps were utilised as a information acquisition and illustration tool among multiple domain consultants within the translation from a press release of needs to style demand specifications. 3 specific goals for this analysis were as follows: demonstrating however idea maps may be used for information acquisition among multiple domain experts; developing a paradigm information illustration model from the idea maps for guiding the event of style needs from "Statements of needs on Orbit"; and assessing the utility of that paradigm information acquisition and illustration model by examination of a restricted drawback set. Kramer was able to effectively show the quality of idea maps in eliciting and representing knowledgeable knowledge; consequently, this paper explores the chance of utilizing idea maps within the digital forensics domain. a prospect exists for incorporating idea maps into each part of a digital investigation; but, during this analysis, idea mapping are going to be applied solely to the examination part of associate investigation.

2. THE IDEA MAPPING CASE DOMAIN MODELING APPROACH

Abstract models square measure appropriate for representing the data domain of a pc forensics examination. idea maps square measure a sort of abstract model that organizes and represents information hierarchically by showing the relationships between ideas. idea maps were initial employed in 1972 to trace and higher perceive children's information of science [22]. Since then, researchers and practitioners from numerous fields have used them as analysis tools, to set up curriculums, to capture and archive knowledgeable information, and to map domain data [21] [22][23]. Novak and Cañas expressed that "concept mapping has been shown to assist learners learn, researchers produce new information, directors to raised manage organizations, writers to put in writing, and evaluators assess learning." moreover, an inspiration map may be viewed as a "simple tool [that] facilitates purposeful learning and also the creation of powerful information frameworks that not solely allow utilization of the information in new contexts, however additionally the retention of information for long periods of time" [22]. In alternative words, data that's learned through the utilization of idea maps permits one to relate this data to previous and doubtless new data and retain this data longer. idea mapping is appropriate for modeling the case domain as a result of idea maps square measure simple to know, may be wont to organize data, features a semiautomated tool offered, may be shared, has the power to make new information and uncover gaps in a very person's information. The idea mapping case domain modeling approach (CMCDMA) was developed from Bogen's [24] case domain model and also the idea mapping model employed by Novak and Canãs [22]. Bogen's [24] case domain model provided a framework for analyzing case details by filtering necessary forensic-relevant case information; additionally, it provided a foundation for organizing information and focusing a forensics examination set up, and it utilised established metaphysics and domain modeling strategies to develop the framework of the model, and computing and software package engineering ideas, like Unified Modeling Language (UML) abstract diagrams, were wont to represent the model. The idea mapping model provides some way to arrange the case details of associate examination, that can be helpful later for analyzing the significant findings. components of each models were wont to produce a 5 part, non-linear method for modeling the data domain consisting of the subsequent steps: distinguishing a spotlight question, distinguishing the case ideas, distinguishing the attributes, distinguishing the relationships, and instantiating the model. First, the main target question is made. the main target question helps give the context for the map to assist in sorting out proof and sorting out extra proof. Second, the case ideas or keywords square measure known. Nouns and noun phrases or objects or events square measure usually chosen to represent the case data. General and specific ideas may be created and employed in future investigations. ideas may be reused from previous cases/models; reusing the ideas will save time once developing future cases/models. Figure one provides a illustration of the idea mapping case domain model for a murder-gambling case.

From this idea map, a general, fast summary of the case is shown. once the preliminary map has been created, the attributes from the case situation ought to be established. Attributes facilitate clarify the concepts' meanings, represent specific events or objects, and might be used for constructing keyword searches, examining documents, examining network logs, and linking alternative ideas [24]. Next, the relationships square measure known. They show however the ideas square measure associated with each other and include verb, verb phrases, numbers, and symbols. within the last part of the CMCDMA, the model is instantiated by adding the attributes, or the particular data, to the map like the name of the victim, the kind of automotive driven by the victim, and also the date the last car care was performed as shown in Figure two. Attributes also

can embody icons like photos, documents, video, audio clips, and alternative digital media. Figure three represents associate instantiated keyword idea map containing the attributes of the murder-gambling case situation with icons displayed for the could Doe and Honda Accord ideas. every of the figures was created victimisation idea mapping software package, CmapTools. The idea mapping case domain model isn't dependent on the CmapTools software package. This model may be made while not the utilization of CmapTools. However, it might be terribly helpful within the enforcement community for as well as extra resources like photos, subpoenas, search warrants, and examination search procedures used.

Not solely will the CMCDMA be wont to organize the case details or manage the information of associate investigator's report, the approach may be wont to structure the examination method additionally. for example, Figure four provides a general examination idea map which will be wont to guide the examiner throughout associate examination. Special techniques steered by the examiner may simply be more to the map and employed in future examinations yet. provided that every case is totally different, a unique set of tasks is also needed to look for associated establish proof in an investigation. This map may simply be altered to incorporate extra tasks pro re nata by following the steps of the CMCDMA.

3. EXPERIMENTAL

style the topic population consisted of enforcement officers taking associate investigation designing category offered through the National Forensics coaching Center. Four experiments were performed. They were divided into an impact cluster and experimental cluster. The experimental cluster used the idea mapping case domain modeling approach. The management cluster failed to use the idea mapping case domain modeling approach however used the widely used, unintended methodology. every cluster used their several strategies to develop keywords, set up and execute the examination, and record the results. the information within the following tables was collected from the experimental data of the management and experimental teams. the info within the following tables solely presents the info provided by the experimental cluster. This information was classified supported the expertise levels of the themes.

subjects' expertise with pc rhetorical examinations had on their skills to use the idea mapping case domain modeling approach to set up, search, and establish proof within the digital rhetorical examination. the general quantity of proof found and time spent within the phases was compared between those with very little or no expertise and people with expertise.

In order to conduct the examination, forensics software package was wont to search and establish proof utilizing the keywords and idea maps created from the idea mapping case domain modeling approach and also the examination idea map. This proof was bookmarked and enclosed within the final report. pc rhetorical software package, like FTK, allowed the case examiner to produce additional/important notes concerning the bookmarked proof additionally to time and date data and also the location of the proof. For this approach, the bookmarked data was wont to indicate what proof was found and wherever the proof was found. Once all the keywords had been searched and also the examiner had completed his/her examination of the proof drive, a report was generated as well as all of the bookmarked things created by the examiner. once the report had been created, a outline report was stuffed out.

4. EXPERIMENTAL ANALYSIS

The data for these applied math analysis tests were taken from the experimental teams of the four experiments. The experimental cluster information was sorted into 2 categories: very little or No expertise (LNE) and full-fledged (E). The LNE cluster consisted of 4 subjects and also the E cluster consisted of seven subjects. the info for experiments 1-4 was combined and analyzed per the teams. for example, in Table 2, E3E-2 represents experiment three and experiment cluster subject two. Table two represents the info collected throughout the look and examination efforts in Experiments 1-4, wherever time is expressed in minutes. Time information data was provided for every subject within the experimental teams (concept mapping case domain modeling approach) for every experiment. during this analysis, subjects with very little or no expertise had 0-2 years expertise in pc rhetorical examinations; additionally, those subjects with over two years expertise in pc forensics examinations were thought of full-fledged.

REFERENCES

[1]. V. Baryamureeba, F. Tushabe. "The increased Digital Investigation method Model". In Proceedings of the fourth Annual Digital rhetorical analysis Workshop, Baltimore, MD, 2004
[2]. N. Beebe and J. Clark. "A gradable, Objectives-Based Framework for the Digital Investigations Process". In Proceedings of the fourth Annual Digital rhetorical analysis Workshop, Baltimore, MD, 2004

[3]. B. Carrier and E. Spafford. "An Event-Based Digital rhetorical Investigation Framework". In Proceedings of the Fourth Annual Digital rhetorical analysis Workshop, Baltimore, MD, 2004
[4]. S. Ciardhuáin. "An Extended Model of law-breaking Investigations". International Journal of Digital proof, 3(1):1-22, 2004
[5]. M. Reith, C. Carr, G. Gunsch. "An Examination of Digital rhetorical Models". International Journal of Digital proof, 1(3):1-20, 2002
[6]. G. Ruibin, T. Yun, M. Gaertner. "Case-Relevance data Investigation: Binding pc Intelligence to the present pc rhetorical Framework". International Journal of Digital proof, 4(1):1-13, 2005
[7]. J. Venter. "Process Flow Diagrams for coaching and Operations". Advances in Digital Forensics II, Springer, pp. 331-342 (2006)
[8]. Tanner and D. Dampier. "Concept Mapping for Digital Forensics Investigations". Advances in Digital Forensics V, Springer, pp. 201-300 (2009)
[9]. Tanner and D. Dampier. "Improving Digital Forensics Investigations with idea Mapping". In Proceedings of the Fifth International Conference on Digital Forensics, Orlando, FL, 2009
[10]. S. Peisert, M.Bishop, S. Karin and K. Marzullo. "Toward Models for rhetorical Analysis". In Proceedings of the Second International Workshop on Systematic Approaches to Digital rhetorical Engineering. Bell Harbor, WA, 2007
[11]. M. Khatir, S. M. Hejazi and E. Sneiders. "Two Dimensional proof reliableness Amplification method Model for Digital Forensics". In Proceedings of the Third International Workshop on Digital Forensics and Incident Analysis. Malaga, Spain, 2008
[12]. Y. Shin. "New Digital Forensics Investigation Procedure Model". In Proceedings of the Fourth International Conference on Networked Computing and Advanced data Management. Gyeongju, Korea, 2008