ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

Digital Forensics Triage for Automated Analysis of Digital Evidence

[1] Shital Gade, [2] Vanita Mane,
[1] Department of Computer engineering, Ramrao Adik Institute of Technology, Navi Mumbai,
[2] Department of Computer engineering, Ramrao Adik Institute of Technology, Navi Mumbai,
[1] gade.sheetal@gmail.com, [2] vanitamane1@gmail.com

Abstract— With the rapid advancements in information and communication technology in the world, the number of crimes related to the digital devices with huge storage space and broadband network connections has increased dramatically and these crimes are becoming technically intensive. It is indeed very crucial for digital forensics investigators to timely identify, analyze and interpret the digital evidence. The digital forensics investigations are carried out to investigate a wide variety of crimes including child pornography, murder, child abductions, missing or exploited persons. In such types of cases, there is a need for timely identification and analysis of digital evidences found at the crime scene. The forensic experts dealing with such crime investigations, need quick investigative leads. The traditional, manually intensive and time consuming procedures indeed, may no longer be appropriate in such cases. There is a need of advanced investigative techniques which can speed up investigation process. The paper explores one of such advanced techniques, 'Triage' which combines the principles of data mining and machine learning. Triage is a technique used in many disciplines, when applied to digital forensics its goal is to speed up the investigation process. Based on the connections between the digital evidences retrieved and crimes under investigation, our proposed triage model aims at automating the categorization of the digital media.

***Index Terms*— Computer crime, data mining, digital evidence, digital forensics, machine learning, triage**

I. INTRODUCTION

Over the past few years, the rapid advancements in information and communication technology in the world has contributed to the increased number of crimes involving digital devices. Today personal computers are so ubiquitous that the collection and use of digital evidence has become a common part of many criminal and civil investigations. A large amount of data or information is generated, accumulated and distributed via electronics means. Computerized evidence requires special handling and analysis as the electronic data can be easily damaged, changed or erased, if handled improperly. Digital forensic examinations expand in proportion to the increase in size of forensic units. In many investigation cases, the digital devices seized at the crime scene contain hundreds of terabytes of data. The forensics experts dealing with such investigations need large amount of time and efforts, in analyzing such huge amount of data but the results produced (i.e. the crime-related evidences retrieved) are not proportional to the time and efforts taken. Traditional techniques of forensic investigation are not appropriate for such growing amount of digital data which require large amount of efforts for analysis . As a consequence, there is a need to reverse this negative trend by using some techniques to narrow the search which can speed the forensics investigation process. There have been various methods developed to deal with wide variety of criminal and civil investigations which constitute growing amount of digital evidences. The paper explores one of such recently emerged technique, called Triage which allows ranking digital media by probative content and quickly identifying the relevant ones.

Triage is a technique used in many disciplines, most notably in the field of medicine as a way of prioritizing injured or ill patients for treatment. It can be viewed as a way of organizing a workload to allow for the efficient allocation of available resources. When applied to digital forensics, its goal is to speed up the investigation process by attempting to identify evidential exhibits and files quicker. The paper describes the 'Triage process model', intended to speed up the digital

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

forensics investigation, which aims at processing seized digital media/evidences and identifying, at an early stage, the most relevant ones from the investigative point of view. The proposed Triage process model combines the principles of data mining and machine learning. The model is able to prioritize all the available digital evidences based on the crime dependent features such as file statistics, browser history and installed applications i.e. the digital devices with high crime related relevance will be categorized as suspicious. Based on the connections between the digital evidences retrieved and crimes under investigation, the proposed model aims at automating the categorization of digital media.

II. RELATED WORK

A new "live" forensics methodology called Computer Forensic Field Triage Process Model (CFFTPM) has been proposed by Rogers M. K. et al. [3], a field or on-site approach for providing timely identification and analysis of digital evidence(s). The computer forensics field triage process model involves the field analysis of the computer system i.e. the model can be applied at the crime scene without the need of transporting the digital device(s) to the lab for acquiring the forensically sound image or for the detailed analysis of the seized digital device(s). The computer forensics field triage process model supports to the traditional forensic principles and its on-site/field approach provides the benefit of minimizing the contamination or tampering of the original evidence and scene, maintaining the integrity of digital evidence. The Computer Forensic Field Triage Process Model has been used in various real world cases successfully and furthermore, the derived evidence from these cases has not been challenged in the proceedings of court where it has been introduced.

Veena H.B. et al. [4] proposed a new approach for data extraction, storage and analysis of data retrieved from the digital device(s) which can be used as a evidence in the forensic investigation. A data mining approach has been used for data generation and analysis and a machine learning statistical approach is used in validating the reliability of the pre-processed data. Authors have focused on proposing an alternate framework for investigation process of physical storage devices, which builds on the models already proposed and chalks out the implementation process for extraction and preprocessing of data extracted from a flash drive. The framework is easy to implement and scientifically practical in approach. It involves six stages: Preparation, Collection and preservation of digital device, Data extraction and preprocessing, Data examination and analysis, Reporting and documentation, Presentation in the court of law. The data extraction and preprocessing phase has been tested out for effectiveness and discussed in detail in their paper.

Marturana et al. [6] have proposed a Triage model for content based classification of digital media and presented the results of a case study in which the methodology was tested against forensic data from court cases of copyright infringement. Their research aims to add new pieces of information to the automated analysis of evidence according to Machine Learning-based "post mortem" triage and the research draws the guidelines for drive-under-triage classification (e.g. hard disk drive, thumb drive, solid state drive etc.), based on a list of crime-dependent features. The model is able to classify evidential exhibits by predicting the class variable according to the aforementioned crime-dependent features.

Fabio Marturana a, Simone Tacconi [7] describe a Triage-based model for crime-related and content-based classification of digital media and present the results of two case studies in which the methodology was tested against forensic data from court cases of copyright infringement and child pornography exchange . Their proposed model is applicable for both "live" and "dead" digital forensics investigations. The stepwise procedure for their proposed model is as follows: (i) defining a list of crime-related features, (ii) identification and extraction of these features from available devices and forensic copies, (iii) populating an input matrix (iv) processing it with different machine learning mining schemes to come up with a device classification. The methodology aims at processing the digital media and identifying the most relevant data for investigation. The popular mining algorithms like Bayes Networks, Decision Trees, Locally Weighted Learning and Support Vector Machines have been used for device classification and the benchmark study about these algorithms has been performed to find out best performing ones.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

III. PROPOSED TRIAGE MODEL

The proposed Triage process model is shown in Fig. 1. The model involves four stages : Evidence Acquisition, Feature Extraction, Find Suspicious Evidences, Triaging.

Evidence Acquisition, the first stage of the process is in charge of creating a forensic image of the seized media/device(s). Extreme care needs to be taken at this stage as digital evidence can be damaged, altered or destroyed by improper handling. This stage of the process is aimed at securing all the seized digital devices to prevent tampering and to preserve the integrity of the digital evidence.

The next stage of our workflow, called **Feature Extraction** is tasked of extracting the crime's dependent features e.g. the number of installed software or the media files average size, file timestamps i.e. file creation time, access time, modification time etc., from each seized drive and creating the data-set. The sample list of features which could be extracted from the seized drives is given below:

- Document or pdf files, average file size, creation time, access time, modification time
- Video or music files, average file size, creation time, access time, modification time
- Type of picture files, average file size, creation time, access time, modification time
- Compressed files, average file size, creation time, access time, modification time
- ISO files, average file size, creation time, access time, modification time
- HTML files/category of visited URLs (illegal/copyright urls, hacking)

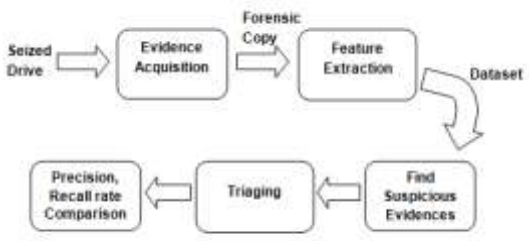

Fig. 1: Triage Process Model

The next stage **Find Suspicious Evidences** is aimed at finding the suspicious evidences. Each seized drive is analyzed for (i) the crime related evidences available (ii) time slots during which applications or files are accessed (iii) the modifications/alterations done to the original data. In our model we take into consideration document files, compressed files, image files, pdf files, media files, html files. A particular procedure is followed to analyze the modifications done to respective files. Once the above examination is done, the dataset is created which contains the information about the crime related evidences, modification to the original data etc. along with the timestamps. The suspicious evidences or features found are then processed or categorized in the next stage.

The **Triaging** stage is in charge of mining the dataset matrix retrieved in the previous stage, to provide a categorization of each device, on the basis of the crime-related relevance of its content. This stage provides classification of the data-set by processing it with Naive Bayes Classifier. Naive Bayes classifiers are highly scalable, requiring a number of parameters linear in the number of variables (features/predictors) in a learning problem. Naive Bayes classifiers can be trained very efficiently in a supervised learning setting and known to outperform even highly sophisticated classification methods. The dataset matrix retrieved in the previous stage is processed with Naive Bayes classifier which provides the categorization of the seized digital devices as 'suspicious' or 'non-suspicious'. The classifiers performance is then measured using the following performance indicators: precision, recall, f-measure, accuracy and false positive rate.

IV. PERFORMANCE EVALUATION

Classifier's learning effectiveness is evaluated according to the following performance indicators: Precision, Recall, F-measure, Accuracy and False Positive Rate defined respectively as:

***Precision*:** In a classification task, the precision for a class is the ratio of the number of relevant records retrieved to the total number of relevant and irrelevant records retrieved i.e. the number of true positives divided by the total number of elements labeled as belonging to

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

the positive class (i.e. the sum of true positives and false positives). Precision corresponds to the proportion of the predicted positive cases that were correctly classified.

Precision = TP / (TP + FP)

***Recall*:** Recall is the ratio of the number of relevant records retrieved to the total number of relevant records in the database i.e. the number of true positives divided by the total number of elements that actually belong to the positive class (i.e. the sum of true positives and false negatives).

Recall = TP / (TP + FN)

***F-measure*:** In classification tasks, the f-measure that combines precision and recall is a measure of test's accuracy. F-measure is the weighted harmonic mean of recall and precision.

F-measure = 2*Recall*Precision / (Recall + Precision)

Where TP=True Positive, FP=False Positive and FN=False Negative.

The above measures are used to evaluate how satisfactory are the evidences retrieved by the system and thus, suit the purposes of this research. To measure the overall classifier performance the Accuracy and False Positive Rate of the classifier can be calculated.

Accuracy: It represents the success rate of the classification algorithm and corresponds to the number of correct classifications divided by the number of documents.

Accuracy = (TP + FN) / (TP + FN +FP + TN)

***False Positive Rate*:** In addition to the accuracy, the false positive rate FPR corresponds to the rate of incorrect classifications made by the system.

FPR = FP / (FP + TN)

The implementation is based on a collection of data extracted from 8 seized digital devices which includes 5 hard drives, 2 tablets and a pen drive. The crime-related features are extracted from the forensic copy of the seized drives and creating a dataset. Each seized drive is analyzed against the modifications done to the original data to find out the suspicious evidences. Based on the crime-related relevance indicator, the dataset matrix is processed with Naïve Bayes Classifier in order to provide a device categorization (suspicious or non-suspicious). The classifier's learning effectiveness is evaluated according to the following parameters: Precision, Recall, F-measure, Accuracy and False Positive Rate. The experimental results are summarized in Table 1.

Table 1: Performance Evaluation

Performance Parameter	Naïve Bayes Classifier
Precision	0.947
Recall	0.972
F-measure	0.960
Accuracy	0.840
False Positive Rate	0.285

V. CONCLUSION

The research which deals with the Digital Forensics Triage is potentially applicable to a variety of crime investigation cases where time is a crucial factor i.e. timely identification and analysis of the digital evidence is necessary, as in some cases human life or safety is at stake. Such cases are child abductions, hacking, murder, missing or exploited persons, terrorism. The proposed Triage process model involves following four phases: Evidence acquisition, Feature extraction, Find suspicious evidences and Triaging. The proposed triage methodology predicts the associations among the evidences retrieved and the crimes under investigation. Once applied to the available seized devices, the model identifies the relevant evidences requiring further lab

analysis. The proposed triage model aims at speeding up the investigation process by prioritizing the seized digital devices according the crime-related relevance i.e the digital devices with high crime relevance indicator are categorized as suspicious. Focusing on the suspicious digital devices for analysis, speeds up the investigation process which would have been a time consuming activity, if done manually.

REFERENCES

[1] Vassil Roussev, Candice Quates, Robert Martell, "Real-time digital forensics and triage", Digital Investigation, Sept. 2013.

[2] Richard E. Overill a,J antje A.M. Silomona, Keith A. Roscoe, "Triage template pipelines in digital forensic investigations", Digital Investigation, Sept. 2013.

[3] Rogers, M. K., Goldman, J., Mislan, R., Wedge T., "Computer Forensics Field Triage Process Model", Conference on Digital Forensics, Security and Law, 2006.

[4] Veena H Bhat, Abhilach R. V., P. Deepa Shenoy, Venugopal K.R., L.M. Patnaik, " A Data Mining Approach for Data Generation and Analysis for Digital Forensic Application", IACSIT International Journal of Engineering and Technology, Vol.2, No.3, ISSN: 1793-8236, June 2010.

[5] Bertè, R., Marturana F., Me G., Tacconi S., "Data mining based crime dependent triage in digital forensics analysis", Proceedings of International Conference on Affective Computing and Intelligent Interaction (ICACII 2012) and IERI Lecture Notes in Information Technology ISSN: 2070-1918, in press , Feb. 2012.

[6] Fabio Marturana, Rosamaria Berte, Simone Tacconi,Gianluigi Me, "Triage-based automated analysis of evidence in court cases of copyright infringement", First IEEE International Workshop on Security and Forensics in Communication Systems, June 2012.

[7] Fabio Marturana a, Simone Tacconi, "A Machine Learning-based Triage methodology for automated categorization of digital media", Digital Investigation 10, Sept. 2013.

[8] Marturana, F., Berte R,; Me G., Tacconi S., " Mobile Forensics "triaging": new directions for methodology", Springer ISBN: 978-88-6105-063-1, Proceedings of VIII Conference of the Italian Chapter of AIS (ITAIS 2011) Rome, Italy, 2011.

[9] D. Bem, F. Feld, E. Huebner, O. Bem, "Computer forensics — past, present and future", Journal of Information Science and Technology 5(3), 2008.

[10] Graeme Horsman, Christopher Laing, Paul Vickers, "A case-based reasoning method for locating evidence during digital forensic device triage", Decision Support Systems, May 2014.

[11] Robert J. Walls, Erik Learned-Miller, Brian Neil Levine, "Forensic Triage for Mobile Phones with DEC0DE", Digital Investigation, 2012.

[12] Inikipi O. Ademu, Dr Chris O. Imafidon, Dr David S. Preston, "A new approach of digital forensic model for digital forensic investigation", International Journal of Advanced Computer Science and Applications, Vol.2, No.12, 2011.

[13] P.A. Aguileraa, A. Fernández b, R. Fernández a, R. Rumí b, A.Salmeronb, "Bayesian networks in environmental modelling", Environmental Modelling and Software 26, 2011.

[14] C.Ramasubramanian, R.Ramya, "Effective Pre-Processing Activities in Text Mining using Improved Porter's Stemming Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013.

[15] Yunus Yusoff, Roslan Ismail, Zainuddin Hassan, "Common phases of computer forensics investigation models", International Journal of Computer Science and Information Technology (IJCSIT), Vol.3, No.3, June 2011.

[16] W.A. Awad, S.M. ELseuofi, "Machine Learning Methods for Spam E-Mail Classification", International Journal of Computer Science and

Information Technology (IJCSIT), Vol.3, No 1, Feb. 2011.

[17] Ira Cohen, Nicu Sebe, Fabio G. Cozman, Marcelo C. Cirelo, Thomas S. Huang, "Learning Bayesian Network Classifiers for Facial Expression Recognition using both Labeled and Unlabeled Data", Proceedings 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Vol. 1, June 2003.