J. Appl. Environ. Biol. Sci., 4(9S)205-209, 2014

© 2014, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental
and Biological Sciences
www.textroad.com

Case Oriented Digital Evidence Similarity Framework

Muhammad Ilyas, Rida Zahra

University of Sargodha, Sargodha, Pakistan

Received: September 12, 2014
Accepted: November 23, 2014

ABSTRACT

In this paper a new framework is present, named case oriented digital evidence similarity framework (CODES). This framework is a top down approach, consists of tasks basically starting from the arrival of new crime case, mainly cyber crime, till the generation of final report regarding that case. This framework facilitates the investigation of a cyber crime case by matching the digital evidences collected from new cases to the digital evidences of previous case thus abstracting the crime pattern of the cases which makes it easy to reach the criminals or unscrupulous individuals. By using CODES framework investigators will be able to use already stored digital evidences to find the similarity in current and previous evidences thus making it easy to trap the criminals and saving time.

KEYWORDS: Digital Forensic, Forensic Computing, Digital Evidence, Similarity, Top down Approach, Cyber crime.

1 INTRODUCTION

To deal with digital forensic analysis is becoming difficult as the complexity of cases is increasing day by day, abundant of data, and advancement in the technology [1]. Investigators face large number of problems in making an obvious start point from where they can start their first step. If investigators start to collect digital evidences and match them with the concept of similarity which is a widely used concept in computer software engineering then it will be easy for investigator to solve same alike cyber crime cases. The concept of similarity emerged as a strong concept in computer science fields and is used in many different aspects [4]. The concept of Similarity is basically come from psychology, in which it is told that how different kind of data and information can be merged in form of group or classes [5, 6].

Computer forensics (CF) has transform as a strong concept in the past some years. Computer forensics play a very vital role in law enforcement especially cyber laws because it helps in collecting the digital evidences of cyber crime [2].

The work is organized in the following sections. Section 2 describes a small comparison between forensic science and computer forensic and some about Digital Forensic and its branches. Section 3 describes similarity and its use in various facets of the field. Section 4 introduces CODES framework and its description. Section 5 contains conclusion and future work.

2 COMPARATIVE ANALYSIS OF FORENSIC SCIENCE AND COMPUTER FORENSIC

With the advancement of internet technology and use of computer in every aspect of life, misuse of it goes with it as well. Computer forensic has come into being in dealing with this situation, the growth and advancement in this field is not much fast as it is new. Forensic has evolved over the past millennium and computer forensic has evolved over the past years which is being active in much from the year 2005. The current research and study in computer forensics is focusing on how to derive a single case from two parts. Computer forensics has been facing a very similar situation like forensic science in which it was difficult to expound scientific evidences in court. Well understanding of scientific evidence and digital evidence by the law enforcement organization is necessary to evolve and advance computer forensic and forensic science.

2.1 Digital Forensics

Digital forensics or digital forensic science is come into being from forensic science and it is used to solve the cyber crime cases especially helpful to find the digital evidences and investigating them. In

*** Corresponding Author:** Mr.Muhammad Ilyas, University of Sargodha, Sargodha, Pakistan
m.ilyas@uos.edu.pk,

addition to find the digital evidences from the crime case itself it can also be used for specific purpose like, determining the intent of crime being done, identify sources (for example, in copyright cases), or authenticate documents. The scope of investigation has become broader as compared to other areas where investigation was just answering a series of simple question. [7].
Digital forensic can be divided into three broad categories [3]:

- Computer Forensic
- Network Forensic
- Cyber Forensic

Computer Forensic Computer can be used to commit crimes, and crimes can be recorded on computers. These crimes include company policy violations, embezzlement, e-mail harassment, murder, leak of proprietary information and even terrorism. Law enforcement agents, network administrators, and private investigators are now relying on the skills of professional computer forensic examiners to explore criminal and civil cases. In general, a digital forensic expert investigates data that can be retrieved from computer hard disk or other storage medium, just like an archaeologist excavating site. Computer forensic is evolving as a strong field and many researchers are working on it.

Network Forensic Network forensic can be divided into two different streams. First is related to security where we continuously monitoring inconsistent network traffic and identifying intrusions. People who done crime through network use different system to commit crime which cause a unusual network usage pattern which is traced to investigate the cases. Second is related to law enforcement in which we can analyze the capture or recorded information and try to produce digital evidence, which we can be used in legal proceedings. Digital evidences are the most important thing in digital crime investigation. As most digital type crime is done through networks so network forensic is becoming important in digital crime investigation.

Network Forensic Cyber crime investigation uses digital evidences to give a meaningful description of the unusual cyber activities. As there are many benefit of cyber technologies which are helping human being in many aspects of life the negative use of it also exist there which shows the bad picture of cyber technology which actually is not true. That is why Cyber forensic is a widely use term now a days for the enforcement of laws [8]. The use of digital data for inclusion into a criminal investigation is also included in cyber forensics. As the involvement of computers in crimes is increasing day by day, many technologies related to cyber forensic are being developed to overcome this.

3 SIMILARITY

Similarity is a vast concept which is used in many disciplines in different aspects to get benefit from it. In the field of computer sciences many researcher and authors have use this concept in different branches of computer science like in artificial intelligence it is used to see the similarity between different groups of data, in software engineering it is used to see similarity between requirements, in network security and so on. Similarity plays a helpful role when there is large amount of data and it is to be grouped together to make comparison [5, 6]. Many researchers have used the concept of similarity in fusion with other concept mostly in artificial intelligence like text base similarity, speech recognition and clustering. It has also been used in many concept of software engineering like requirement base similarity and many more [9].

4 CODES FRAMEWORK

The CODES Case Oriented Digital Evidence Similarity Framework is presented in fig given below. This framework is a top down approach. Different stages from start to end are mentioned which are grouped as, Case, Digital Evidences, Digital evidence repository and final report generation. This framework will help the investigators in saving time by shorten the timeline of investigating the case by matching the digital evidences of the case.

4.1 Top down Approach

The top down approach is used when the whole process goes in a smooth process from starting till end. In CODES framework top down approach is used because the investigation is started from the top from the arrival of the case and then the middle part; analysis of case for collecting digital evidences; checking the similarity of new evidences with previous till final report generation. In contrast to this bottom up approach use different strategy in which it start from the end and going to the up.

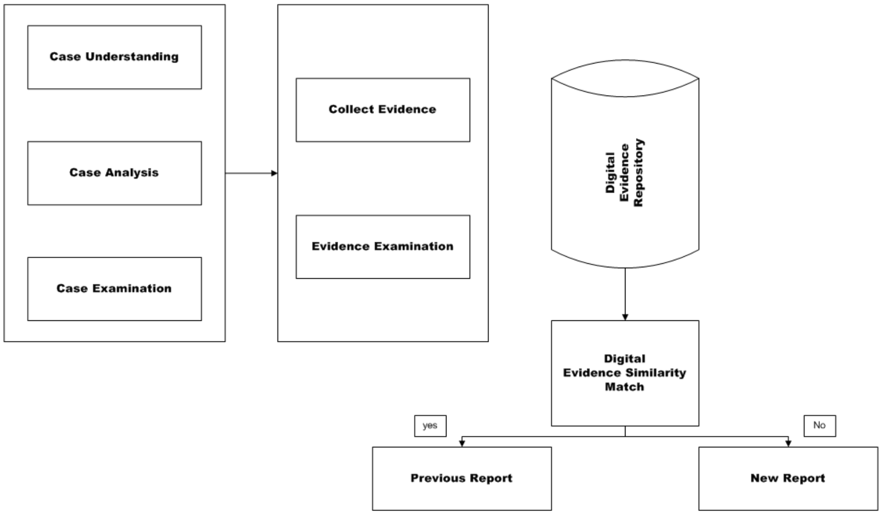

Figure1. Case Oriented Digital Evidence Similarity Framework (CODES)

4.2 Case Oriented Phases

First CASE level includes two CASE-oriented phases; Case Understanding, Case analysis and Case examination. When the new case is arrived it will deeply examined by the investigator to understand the nature of crime and somehow the motivation of the criminal. It is very important to understand the nature of case because through this the investigation team will be able to collect the digital evidences. As cases can are of two type which are

- Public sector cases
- Corporate or private sector cases

Public sector cases are those in which government agencies are included as criminals in investigation. Public sector cases also demand the investigator to understand the place where the crime has been done. Other type which is in cooperate or private sector cases which include crimes related to private organization and companies. This type of cases demands the investigator to understand the business and also requires that the business do not get disturbed during this investigation. After fulfilling these requirements, the case is analyzed in the third phase. The dimension of the crime done through computer is some time same and some time different like there are many crime cases like fraud, bomb blast, kidnapping, hacking, embezzlement, smuggling of drugs, hijacking and other like that. So it is very necessary to deeply understand, analyze and examine the case.

4.3 Collection of Digital Evidences

Digital evidence is the most important thing when investigating for a crime which is committed using computers or other digital devices. This evidence is the only thing which is presented in the court by investigators. The nature of digital evidences varies between different operating system when it comes in term of computer and other digital devices such as mobile phone etc. It is very tricky job for investigators to collect the digital evidences as well as saving them for use in future in other similar cases decreasing the cost use per case and also the time. In the second phase of the framework which is the collection of digital evidences the case is examined to collect the evidences with respect to the following facts what, Why, Who, Where, When, How. These facts will help in collecting the digital evidences of the crime case and will also be saved in the repository. The collected evidences will be examined to find out the pattern of crime. It is seen in many cases that most criminal groups, hackers and individual doing crime through network mostly use the same patterns.

In CODES framework the digital evidences will be collected category wise like with respect to the nature of crime done and saved in the repository attribute wise so that it will be easy to apply similarity check on them. These attributes include digital evidences with respect to time, place, person and some more. Saving digital attributes like this will help in matching similarity of new and old digital evidences.

4.4 Digital Evidence Repository

Digital evidences are easily altered, duplicated and erased if not kept safely. In cyber crime case these are the only thing which is presented in front of court during the hearing of case. Keeping this in mind a digital evidence repository is presented in the framework. All the evidences new or old will be saving in it. The identified digital evidences of the crime are sending to the digital evidence repository where digital evidences of previous crime are saved. This will help in matching the current evidences with the previous ones to see that is there any similarity between the evidences with respect to any fact which may be time, person, place, procedure etc. if there would be any similarity the investigator will try to find the connection with the previous crime cases, if not then the team of investigation would go for new strategy and generate a new final report.

4.5 Digital Evidence Similarity Match

Digital evidences are easily altered, duplicated and erased if not kept safely. In cyber crime case these are the only thing which is presented in front of court during the hearing of case. Keeping this in mind a digital evidence repository is presented in the framework. All the evidences new or old will be saving in it. The identified digital evidences of the crime are sending to the digital evidence repository where digital evidences of previous crime are saved. This will help in matching the current evidences with the previous ones to see that is there any similarity between the evidences with respect to any fact which may be time, person, place, procedure etc. if there would be any similarity the investigator will try to find the connection with the previous crime cases, if not then the team of investigation would go for new strategy and generate a new final report.

4.6 Report Generation

Final report generation matters a lot at the end of whole process because it will tell the investigator that in what direction now the team has to proceed. There can be two types of report generated at the end is totally new repot and the other one will be the updated report. The report generation regarding whole investigation is based on the digital evidence match who is done with similarity match. New report with new facts and investigation will be generated if there is no similarity between current and previous digital evidences of crime cases. This report will contain all new facts, digital evidences, facts and figures regarding new crime case. If any similarity between attribute of current and previous digital evidence is to be found the report will be generated in accordance with that.

5 CONCLUSION AND FUTURE WORK

This work presented a case oriented digital evidence similarity framework CODES, whose purpose is to find out similarity between the digital evidences of different cyber crimes. The two main purpose of this framework are, one to match the digital evidences of current crime case with the digital evidences of already solved crime cases, to see that they have similarity in them and based on this fact second objective is to save time and effort by solving the case at hand.In future this framework will be implemented practically in the form of tool or running application to get more benefit from it. That tool will be practiced on real time digital crime cases to make a beneficial use of it.

REFERENCES

1. Jun Zhang, Lina Wang, “Application of Case-oriented Evidence Mining in Forensic Computing”, International Conference on Multimedia Information Networking and Security 2009.
2. Ryan Hankins, Tetsutaroh Uehara, Jigang Liu, “Comparative study of Forensic science and Computer Forensics”, Third IEEE International Conference on Secure Software Integration and Reliability Improvement 2009.
3. Ankur Kumar Shrivastava, Nitisha PAyal, Archit Rastogi, Amod Tiwari, “Digital Forensic Investigation Development Model”, 5th International Conference on Computational Intelligence and Communication Networks 2013.

4. E. L. Rissland, “Artificial Intelligence and Similarity”, IEEE Intelligent Systems 2006; 21(3):39-49.
5. R.L. Goldstone and J. Son, “Similarity”, In K Holyoak and R. Morrison, editors, Cambridge Handbook of Thinking and Reeasoning, Cambridge University Press 2005.
6. D. Medin, R. Goldstone, D. Gentner, “Respects for similarity”, Psychological Review 1993; 100(2):254-278.
7. http://en.wikipedia.org/wiki/Digital_forensics
8. http://www.webopedia.com/TERM/C/cyber_forensics.html
9. Muhammad Ilyas, “A similarity Measurement Framework for Requirement Engineering”, Fourth International Multi-Conference on Computing in the Global Information Technology 2009.