ISSN (Online) : 2249 - 054X

International Journal of Computing and Corporate Research

Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M14-052013

VOLUME 3 ISSUE 3 May 2013

OUTLIER ANALYSIS IN FORENSIC DATABASES AND CYBER INVESTIGATION

Pavan Kumar Doppalapudi [1] Research Scholar,
Shri Venkateswara University ,Gajraula, Amroha (Uttar Pradesh)

Dr. Sohan Garg [2] Director, S.C.R. Institute of Engg. & Technology.
(C.C.S. University Campus, Meerut)

Abstract:

Forensic examination plays big role in the modern computer security,due to the sheer amount of data involved and involving the complexity of computer systems **.***In trendy society computers have taken a central position in several aspects of human lives. Computers are employed in education, banking, communication, transport, security, administration and plenty of different spheres of life. Similarly, crimes involving computers and computer application have additionally increased along with the advancement of the computer technology. This has necessitated the institution of a branch of rhetorical science to manage this rising style of crime. This branch is what's currently mentioned as computer rhetorical.*

This branch of rhetorical science deals with the gathering and analysis of digital database with the aim of providing proof that may assist in resolution against the law (Craiger, 2006). There are numerous computer rhetorical techniques. The main ones include; cross drive analysis, live analysis and deleted files recovery. There also are numerous classes of computer rhetorical proof.

Three broad classes are coated during this paper. These are; mobile devices, network rhetorical and database rhetorical. so as to confirm that proof gathered through computer rhetorical techniques is admissible in court, there are sure issues that has to be adhered to. These issues have additionally been self-addressed herein.

1. INTRODUCTION

Computer rhetorical may be a branch of rhetorical science that principally deals with computer proof (Craiger, 2006). Computer rhetorical techniques involve examining digital media with the aim of protective, convalescent or analysing rhetorical info. Since late twentieth century computers became distinguished in terribly several spheres of life. Through computers criminals will currently gain access to individuals and organization sensitive info, concerning individuals wherever about and monitor people's movement with ease.[24]

This has created the computer a target for several crimes like fraud and hacking. The computers have additionally provided a media through those criminal activities like underage creation, cyber stalking, rape seizure and murder are created easier to commit (Carson, 2010). Computer rhetorical techniques doesn't solely involve examining computer crimes however also are wont to offer proof for different sorts of crimes. This was created attainable in 1980 once digital proof became admissible in court. Since then computer rhetorical techniques are used as sources for providing proof for crimes committed.

Many ancient crimes are currently being assisted or abetted through the employment of computers and networks, and wrongdoing antecedent never notional has surfaced as a result of the unimaginable capabilities of data systems. Computer crimes are requiring enforcement departments generally and criminal investigators specially to tailor an increasing quantity of their efforts toward with success characteristic, apprehending, and helping within the fortunate prosecution of perpetrators. Within the following text, key analysis findings within the space of ancient Yankee criminal investigations are summarized. Similarities and variations between ancient and computer crime investigations are then given, and subsequent implications are mentioned. Pragmatic suggestions on however American computer crime fact-finding task forces will most aptly fulfil their supposed objectives are given lastly via a theoretical example of a specialised unit. It's hoped that past information will be assimilated with current observations of computer-related criminalist to tell and guide the science of police investigations within the future. [1]

2. Criminal Investigation

Criminal investigation has been a subject of study for lecturers and practitioners alike, and is outlined as 'the method of de jure gathering proof of against the law that has been or is being committed' (Brown, 2001:3). It seeks to spot the truths related to however and why against the law occurred, and works toward building a case which will cause the fortunate prosecution of the offender(s). Several analysis studies have wanted to see the simplest means within which the fact-finding method will be conducted and managed. The overarching goal of those studies has been to modify police departments to mirror upon their own practices against the scene of the findings, so to implement salient positive changes which might improve the daily operations of their organization.

Practices of investigation are changed and refined over the years, taking under consideration changes in social, political, economic, and scientific domains. These practices have infused 'science' into an activity that was once primarily thought of an 'art' (Beveridge, 1957), and have consequently increased the fact-finding method.

In his law of insertion, archangel Tarde ([1890] 1903) declared that novel sorts of criminal behaviour are fostered through the superimposing of latest practices onto ancient ones, usually through technological advances or innovation. owing to the exponential growth of data technology in trendy society, several ancient crimes are currently being assisted or abetted through the employment of computers and networks, and criminalist until now never planned has surfaced as a result of the unimaginable capabilities of data systems. These computer crimes would require enforcement departments generally and criminal investigators especially to tailor an increasing quantity of their effort towards with success characteristic, apprehending, and helping within the fortunate prosecution of perpetrators.

In order to develop a sound strategy during this regard, it's crucial to find out from past analysis within the space of investigations, and to include into enforcement organizations those policies deemed most fruitful. Within the following text, a outline of the two most important studies on ancient investigations in America is given for the needs of providing a historical and comparative position. Next, similarities and variations between ancient and computer crime investigations are given, and subsequent implications are mentioned in terms of: the role of the first-responding officer and investigator(s); info, The focus of this study is on investigations of:

1) Ancient crimes within which a computer

is employed in an appurtenant manner, and

2) non-traditional or hi-tech crimes within which a computer is that the primary object of, instrument in, or repository of proof associated with, against the law instrumentation, and interviewing; proof

assortment and processing; territorial issues; reactive and proactive strategies; and utility of symbolic investigations. This work concludes with some pragmatic suggestions on however computer crime fact-finding task forces ought to be created and managed to aptly fulfil their supposed objectives. This can be given via a theoretical example of a specialised unit.

2.1 IP address and time in cybercrime investigation

Cyber technology is a particularly sophisticated field and therefore the net is being progressively used as an area to commit crimes victimisation personal computers, still as network-based computers. Though cyber investigation remains within the early stages of its development, the burgeoning use of the net has exaggerated the requirement for digital investigations. The aim of this paper is to extend awareness of the newest in digital comparison for cyber-crime investigation with the studies of IP-address and time in computer systems.

Design/methodology/approach – The approach to raising a cyber-crime investigation is projected in 3 stages: freelance verification of digital clues, corresponding database from completely different sources, and preparation of a sound argument.

Findings – If the police and different authorities don't stay prime of this drawback, they'll lose the battle to regulate this cyber-crime explosion. The paper discusses however Taiwanese police investigate cyber-crime and therefore the expertise is ready to propagate once analysing IP-address and time with crime-case. It’s believed that this projected approach creates a comprehensive guide that gives support and help to crime investigators.

Practical implications – IP-address and time, each indicated during this paper, are the key ingredients to spot the suspect within the starting of investigation works. because the study shows: there's no guarantee that there forever are the “right” proof to prove everything; investigators ought to attempt their utmost to avoid creating mistakes; criminal investigators should realize extra clues and proof to validate their suspicions.

Originality/value – This paper illustrates associate approach to the investigation of cyber-crime within the case of learning IP-address and time. It’s believed that the analysis will with efficiency assist

ISSN (Online) : 2249 - 054X

International Journal of Computing and Corporate Research

Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M14-052013

VOLUME 3 ISSUE 3 May 2013

enforcement officers in addressing ever-increasing cyber-crime by victimisation effective digital proof.

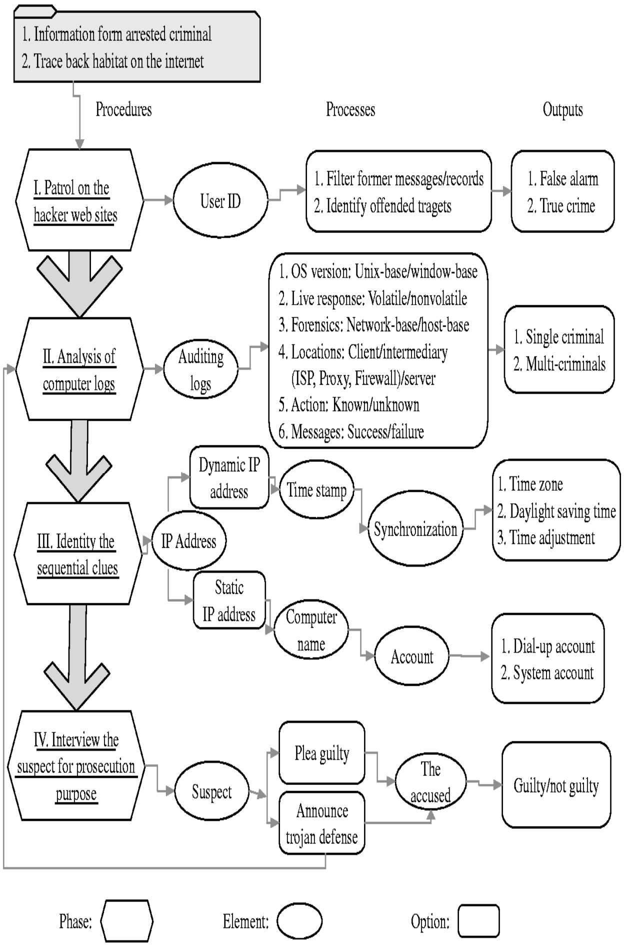
1. Information form arrested criminal
2. Trace back habitat on the internet
Procedures
Processes
Outputs
I. Patrol on the hacker web sites
User ID
1. Filter former messages/records
2. Identify offended tragets
1. False alarm
2. True crime
II. Analysis of computer logs
Auditing logs
1. OS version: Unix-base/window-base
2. Live response: Volatile/nonvolatile
3. Forensics: Network-base/host-base
4. Locations: Client/intermediary (ISP, Proxy, Firewall)/server
5. Action: Known/unknown
6. Messages: Success/failure
1. Single criminal
2. Multi-criminals
III. Identity the sequential clues
Dynamic IP address
Time stamp
Synchronization
1. Time zone
2. Daylight saving time
3. Time adjustment
IP Address
Static IP address
Computer name
Account
1. Dial-up account
2. System account
IV. Interview the suspect for prosecution purpose
Suspect
Plea guilty
Announce trojan defense
The accused
Guilty/not guilty
Phase:
Element:
Option:

Fig 1 crime via IP address

2.2 Rand study of criminal investigation

In the 1970s, the RAND Corporation within the us (US) conducted a nationwide study of criminal investigations by enforcement departments with over one hundred fifty sworn officers or serving a population over one hundred,000. Through analyses of varied agencies with differing fact-finding philosophies, comparison with official crime statistics to see fact-finding effectualness, and a review of careful case studies, a comprehension of however agencies managed and arranged investigations was wanted. Four main conclusions were set forth:

1. **Case answer:** the foremost necessary determinant of case solution was the knowledge provided to the responding officer by the victim (Greenwood, Chaiken, &amp; Petersilia, 1977). it absolutely was additionally discovered that follow-up investigations were mostly ineffective. Specifically, if the victim wasn't ready to offer characteristic database of the offender, it absolutely was unlikely that apprehension would result. The importance of the responding officer highlighted the necessity

for well-trained patrol personnel with a bigger fact-finding role, UN agency are then singularly capable of closing several cases instead of turning them over to a different person (see additionally Block &amp; Weidman, 1975; Joseph Greenberg, Elliot, Kraft, &amp; Proctor, 1977). As a consequence, this might enable specialised fact-finding forces to handle solely those incidents that fully need knowledgeable skills, and would keep their caseload to a manageable size.

2. Fact-finding effectiveness: variations in fact-finding organization, training, staffing, workloads, and procedures didn't proportionately have an effect on crime rates, arrest rates, or clearance rates.

3. The process of physical proof: whereas enforcement departments collected a good deal of physical evidence, abundant of it absolutely was not processed in a good manner. As such, the steered policy concerned the allocation of additional resources to the process of collected proof, which might thereby have a positive impact on crime-solving.

4. Fact-finding thoroughness: Investigators were usually failing to totally document all of the necessary evidentiary facts that may strengthen the flexibility of prosecutors to get the foremost applicable convictions. Wholeness in documentation, it absolutely was argued, might have contributed to a rise within the range of case dismissals and a weakening within the plea bargain position of prosecutors (Greenwood et al., 1977). This deficiency in comprehensive recordkeeping necessitated immediate attention.

PERF Study on the Investigation of felony and theft

In another necessary study light-emitting diode by John Eck below the auspices of the Police government analysis Forum (PERF), more than 3,360 felony and 320 theft investigations over a biennial amount were analysed in 3 jurisdictions: DeKalb County, Georgia; St. Petersburg, Florida; and Wichita, Kansas. The PERF study differed from the sooner analysis by RAND in this it cantered on the complete fact-finding method, instead of solely on the cases cleared by arrest. As such, Eck was ready to confirm the impact of a number of variables that affected the result to disproportionate degrees.

A primary finding was that each detectives and patrol officers contributed equally to the finding of cases, which it absolutely was a ill service to emphasise one over the opposite (Eck, 1983). The analysis additionally found that people in each position ought to be less dependent on database provided by the victim and additional proactive in exploring leads provided by others associated with the incident (Eck, 1983). The follow of neighbourhood bell ringing and also the use of informants were declared as necessary techniques to extend the effectiveness of investigations. It appeared that whereas most databases came from the victims of the crime throughout the initial police response, abundant of these leads were stillborn. once alternative sources were consulted, however, way more helpful database was discovered.

The necessity of being sensitive to victims was additionally underscored by Eck, UN agency declared the relative un-usefulness of re-interviewing the victim throughout follow-up investigations. Physical proof was found to be most helpful to corroborate pre-existing identifications instead of as a method to spot suspects UN agency were antecedent unknown (Sanders, 1977; Wilson, 1976). Cooperation, database sharing, and knowledge management among police departments were additionally extolled as key factors in fortunate investigations (Eck, 1983). one among the foremost sensible recommendations to stem from Eck's study involved the categorization of cases into 3 teams – those who may well be resolved, those who are resolved, and people which will be resolved through some effort (Brown, 2001). This 'triage system' was devised to help enforcement personnel in creating objective choices on that cases were merit resource expenditure. Through this way of case screening, investigations might proceed in a very targeted and enlightened manner when decisive the presence of bound solvability factors that may possibly cause a case clearance. Additionally, this procedure additionally allowed enforcement to tailor their efforts toward the little cluster of habitual offenders or 'career criminals' UN agency commit the bulk of significant crimes (Wolfgang, Figlio, &amp; Sellin, 1972). Eck felt that these suggested changes would go a protracted means in processing the method and rising its utility and success rate.

From these 2 intensive analysis endeavours within the North American country, some necessary lessons will be learned. First, the role of the responding officer is crucial in investigations, and often the knowledge provided to him or her is that the deciding thinks about finding a case. to boot, it seems that increasing the breadth of investigations by exploring alternative avenues of data acquisition might prove valuable, as informative qualitative information will be gained during this manner. Allocating resources solely to those cases possibly to be resolved is another wise strategy that enforcement departments will use. Finally, painstakingness in evidentiary documentation is on the face of it crucial to putting together a robust case and increasing the probability of a fortunate conviction by the prosecuting team.

3 Definitional differences

As mentioned, fact-finding practices and procedures for each ancient crimes and extremely developed sorts of computer crime are similar in several respects just because of a algorithmic method inherent within the modification of ancient crimes through innovation or technological development (Tarde, [1890] 1903). Notwithstanding, important variations exist within the fact-finding method, and these should be accommodated to best address computer crime. These variations are mostly unconcealed by the definitional distinctions in this.

Traditional crimes usually concern personal or property offenses that enforcement has continued to combat for hundreds of years – like the Type I offenses of the FBI's Uniform Crime Report within the North American country. Non-traditional crimes, for the needs of this work, embrace those involving a computer. These traditionally haven't received a proportionate quantity of attention as compared to ancient crimes, despite their gravity and also the substantive hurt they usually cause (Braithwaite, 1985; Hinduja, 2004; Newman &amp; Clarke, 2003; Parker, 1976; Rosoff, Pontell, &amp; Tillman, 2002; Webster, 1980). moreover, they are doing not elicit identical visceral and emotionally-charged reaction from the yankee public and form of government as do the traditional personal and property crimes that police mostly work to handle (Benson, Cullen, &amp; Maakestad, 1990; Cullen, Link, &amp; Polanzi, 1982). Since these entities considerably influence the policies and actions of the North American country criminal justice system, the result's a relatively bit of effort and resources allotted for computer crime. computer crime has been outlined as 'any outlaw act fostered or expedited by a computer, whether or not the computer is an object of against the law, an instrument accustomed commit against the law, or a repository of proof associated with a crime' (Royal Canadian Mounted Police, 2000). a number of the foremost outstanding varieties embrace e-commerce fraud, pornography trafficking, software system piracy, and network security breaches. Fact-finding difficulties are introduced once making an attempt to tackle computer crime as a result of its usually technologically-advanced nature, the very fact that it will occur virtually outright, and since it's very troublesome to look at, detect, or track (Leibowitz, 1999; world organization, 1994; Wittes, 1994). These issues are combined by the relative obscurity afforded by the web likewise because the transcendence of geographical and physical limitations in Internet, each of that render troublesome the detection of criminals UN agency are ready to make the most of a nearly limitless pool of victims.

3.1 Application and extension to computer crime

A multitude of aspects associated with investigations are essentially concerned once considering however ancient practices should be changed, augmented, or maybe restructured to make amends for variations inherent in computer crime. Whereas there's no universally applicable nostrum, it seems that acknowledging and accommodating the subsequent points can lead to bigger fact-finding effectualness once addressing high-technology wrongdoing. Before continuing, though, it should be explicit that whereas this work specifically concentrates on investigations of computer crime, some samples of professional crime which will occur through the employment of computer systems are given to support the assertions.

3.2 Role of the First-Responding Officer

As antecedent explicit, one among the foremost necessary findings of the RAND study involved the role of patrol officers UN agency 1st answer against the law scene. it absolutely was steered that these 1st responders be granted further inquiring responsibilities to ease the caseload burdens of specialised investigators, and since their initial presence on the scene usually gave them database to use as ends up in explore (see e.g., Block &amp; Weidman, 1975; Joseph Greenberg et al., 1977). By extension, the role of the primary responding enforcement officer in computer crime cases is of crucial import as a result of the proof related to a computer crime is usually intangible in nature. Bound precautions should be taken to confirm that information keep on a system or on removable media isn't changed or deleted - either deliberately or accidentally (Lyman, 2002; Parker, 1976). Even the straightforward shutting-down of a computer will modification the last-modified or last accessed timestamp of bound system files that introduces queries related to the integrity of the information. In sum, to preclude vulnerabilities within the prosecutor’s case and to adequately defend against any connected challenges, grave care should be exercised by 1st responders throughout the search and seizure of computer instrumentation. Depicting some parallels to the topic matter at hand is that the assortment of hair, bodily fluids, and covering samples from that DNA is computer crime Investigations within the us – Sameer Hinduja extracted. They need no obvious use or which means till a criminalistics knowledgeable analyses them and consequently determines their rhetorical significance. Once cogent information and proof is obtained from these samples by properly-trained personnel, however, the investigation and its attendant efforts towards achieving justice are usually simplified. in a very similar vein, specialised skills should be schooled to first-responding officers UN agency may encounter technological proof that on the surface might seem hollow however upon additional analyses by computer rhetorical examiners may prove crucial in clearing a case.

3.3 Role of the Investigator

The analysis of timber et al. (1977) explicit that over five hundredth of ancient street crimes are resolved supported database provided to the responding officer by the victim(s), which in cases wherever incomplete or unusable databases provided by a victim, most aren't afterward resolved through fact-finding efforts. Alternative analysis has likewise shown that small is gained through police effort to help in wrongdoer apprehension following the commission of against the law (Block &amp; Bell, 1976; Skogan &amp; Antunes, 1979). Indeed, Skogan and Antunes (1979:223) have specifically explicit that 'investigatory follow-up work, the gathering of physical proof, and also the ferreting out of criminals through police work, play a comparatively unimportant role in characteristic and apprehending offenders.'

Nonetheless, the role of the investigator in computer crime cases are going to be way more necessary in clearance and arrest rates than database given to him or her by the responding officer, victims, or witnesses. Owing to the veiled nature of the techniques related to computer crime and even the particular victimization itself, abundant effort can on the face of it be gone so as to spot evidentiary facts, interpret clues, follow leads, and gather information to form a compelling case against the suspect(s). Additionally, the PERF study suggested that officers work to find witnesses through a locality canvass; the same procedure will be fruitful in an structure context wherever computer crime has occurred.

The scope of the investigation will be dilated to incorporate interviews with alternative persons UN agency may offer qualitative database associated with pressures, demands, constraints, motives, and rationalizations that have an effect on behaviour. Consequently, a way of however the organization shapes and impels behaviour could also be captured, and might thereby assist the investigator in higher comprehending attainable stimuli for crime commission. Info, Instrumentation, and Interviewing O'Hara &amp; O'Hara (1980) have written that there are 3 elements of the criminal investigation: info, instrumentation, and interviewing. Whereas technology and technique may modification, these fundamentals persist across time and are so merit delineation.

Information merely refers to the very fact that criminal investigation is focused round the gathering, organizing, and decoding of information directly or tangentially associated with the case. Second, instrumentation is expounded to rhetorical science and also the specific techniques afforded to crime-solving investigators. For instance, technological advances like biometry, DNA analyses3, and audio/video processing can still enhance the accuracy of enforcement in clearing cases. Third, interviewing involves the method of soliciting and lawfully extracting database from people UN agency are intimate the circumstances of against the law in some capability.

These 3 fundamentals are – and can still be – used within the investigation of ancient offenses within the North American country in a very comparatively simple manner. However, their application to computer crime is a smaller amount clear and on the face of it additional nuanced. Database accumulation can still be the 'bread-and-butter' of the investigation of those non-traditional crimes. In fact, the ability of the investigator is essentially rendered irrelevant if he or she isn't given enough helpful databases to manoeuvre toward case clearance throughout the course of the investigation. Similarly, even the foremost adept investigator can encounter difficulties if database culled throughout its course is incomplete or usually irrelevant. With this in mind, though, instrumentation and interviewing – that are merely alternative ways to assemble database– ought to be dead in a very distinctively completely different manner.

Instrumentation in investigation financially-related crimes involving computer systems primarily revolves round the trailing and analysis of three. Although outside the scope of this work, it's attention-grabbing to think about however the experience of DNA proof assortment and analyses migrated into the police organization, and whether or not the event of that specialised part will function an instructive guide for the introduction and maturation of computer forensics experience.

For example, concealing with the employment of computers issues the method of concealing the supply of illegally-obtained cash and infrequently involves the creation, fabrication, or alteration of documents to make a legitimate written account and history (Lyman, 2002). Monetary establishments are likely to stay careful records of all transactions, currency exchanges, and also the international transportation of funds exceptional a definite quantity. To boot, the Bank Secrecy Act of 1970 needs these establishments to keep up records that 'have a high degree of utility in criminal, tax and regulative investigations and proceedings' and authorizes the Treasury to want the news of suspicious monetary activity which could be associated with a law violation (Office of Technology Assessment, 1995).

Another example testifies to the importance of instrumentation once addressing computer-related wrongdoing. Before the exponential growth of the web, the investigation of credit-card fraud usually concerned correct identification by witnesses and also the assortment and identification of inculpate physical proof. Once a wrong doer created an acquisition at a retail institution through the employment of a dishonourable MasterCard for payment, sales clerks and store workers trained in accurately perceptive and memory physical and activity details of perpetrators were ready to assist within the investigation. Catching a wrong doer in possession of the fraudulently-acquired merchandise was additionally easier since purchases were created in a very physical location. Finally, the handwriting sample obtained once the products were signed for, and fingerprints left at the scene of the crime, additionally served as evidence. With the arrival and growth of electronic commerce, however, the helpful role of witnesses and physical proof – sources of data antecedent (and even heavily) relied upon – has currently been mostly eliminated. Combined with inter-jurisdictional complications, a deficiency of obtainable inquiring resources, and also the proven fact that these crimes occur in such a free and unregulated manner in Internet, the matter is additional perplexed. Investigators of computer crime should consequently pursue alternative avenues of inquiry and learn to master database retrieval from these sources, alternatively still struggle in their case clearance tries.

The third part - interviewing - seems to be less salient as a right away technique to research computer crime, mostly as a result of the victim is usually unaware (either at once or maybe for a good length of time) that against the law has occurred which hurt has resulted (Parker, 1976; Webster, 1980). Database helpful within the finding of those cases is typically solely known when ferreting through reams of information on a ADP system, and infrequently the victim's solely role in these investigations is to report the crime and supply access to the information storage machines. Moreover, witnesses in computer crime are comparatively rare since these offenses tend to occur behind closed doors (Rosoff et al., 2002). The sole witnesses in most cases are people who commit the crimes either severally or jointly, and thus alternative techniques to assemble database should be used (Lyman, 2002).

Interviewing, then, might offer indirect utility for the investigator – like insight into the motives and presumably the precise techniques used, significantly if the wrongdoer wasan‘insider.’ Motive for against the law like peculation (the siphoning off of funds from an leader by a worker – usually through the employment of computer systems (Lyman, 2002; Rosoff et al., 2002)), for instance, may stem from structure variables – like pressure from supervisors or managers to demonstrate productivity or effectiveness, or from a ‘culture of competition’ that permeates the enterprise (Coleman &amp; Ramos, 1998). it would additionally stem from individual-level variables like a temperament characterised by laziness, vindictive inclinations, an inclination to mock authority, or an inability to alter stress in a very pro-social manner (Krause, 2002). Co-workers of an attainable suspect might offer helpful secondary database during this regard, whereas additionally outlining the capabilities of (and ways probably used by) the individual to bypass access controls to commit the crime. The task of the investigator would then be to judge the viability of the anecdotal feedback received, and to follow leads which can uncover stronger proof that may hold substantive weight in a very court of law.

4 Proof assortment and process

In terms of evidentiary problems, the preliminary investigation ways related to computer crime ought to be dead as the other kind of crime. Enforcement departments have procedural necessities for proof assortment that ought to be followed, however bound subtleties endemic to computer crime should be noted. For instance, Lyman (2002) points to the quality related to the dearth of tangible proof and an actual scene to be examined. As such, it's steered that the investigator learn the maximum amount as attainable regarding the victim and also the attainable suspects in a very case. Although not exclusive in their impact, this highlights the prominence of understanding individual-level variables as predictors of this way of criminalist. Moreover, the careful analyses of logs, records, and documents related to the unlawful group action or action should occur (Lyman, 2002). The gathering and use of physical proof has been documented as important (Eck, 1983), and whereas this procedure in investigation computer crime is extremely time-intensive, it usually yields key clues which will cause a terror. The way within which proof is procured in computer crime cases remains a large challenge for enforcement. Specific database associated with the computer system requiring search and attainable seizure should be careful within the warrant so as to be approved, and additionally so the prosecuting officer will counter any evidentiary challenges brought by the defence workers. Consistent fact-finding standards and protocols for computer crimes haven't nonetheless become firmly ensconced in most police departments, and this may cause proof being deemed inadmissible – proof that otherwise might need light-emitting diode to a conviction (Lyman, 2002; Webster, 1980). Warrant proceedings for ancient crimes are acquainted and routine to the room workgroup. Owing to the relative age of warrant applications for computer crimes, however, some states are specifically designating individual judges to alter these specialised requests (New Jersey professional person General Commission of Investigation, 2000). Notwithstanding, requests should still be given in a very manner that enables simple comprehension. The selection should not be confused by the technical details related to the investigation, however ought to perceive the nuances of what's concerned so the court will build an enlightened call. The goal is to obviously articulate grounds that against the law have been committed, which the things delineated within the warrant is associated with that crime. Likewise, technological jargon is usually employed by victims to speak the specifics of the victimization and attainable sources of fact-finding clues, and plenty of enforcement officers themselves might not be ready to absolutely perceive the knowledge, nor assimilate it to direct or refine the investigation (Lyman, 2002). Additional police agencies are using technicians UN agency will assist responding officers or detectives within the correct preservation, collection, and process of proof, likewise like interpretation and presentation of the technological details of crime commission.

Once proof related to a computer crime is lawfully discovered, multiple safeguards ought to be instituted to preserve its continuity and integrity. Extreme attention should be to the specifications on the warrant so all relevant things are properly and de jure appropriated. Moreover, it's predominant to shield physical and removable media as a result of their sensitive nature. Magnetic fields and even electricity have the potential to render unusable and indecipherable bound equipment like information storage devices or disks.

Another crisis is that suspects in a very case ought to be restricted from the computing setting as a result of the likelihood that digital proof can be altered or deleted (Lyman, 2002). At this time, the rhetorical analysis of computer laborious drives has tested to be useful in building a case against a suspected criminal.

5. CONCLUSION AND FUTURE WORK

In this paper we described a methodology to automatically extract expert-system-like if-then rules from forensic databases. The methodology and the algorithms used were proven to be easily implementable in most data analysis environments.

The conducted tests have shown very satisfactory results. They were able to unveil all the hidden structures we were testing them on. The accuracy of the rules inferred was very high and clearly better then the minimum level required to make them usable in a practical setting. However, the tests have also shown a drawback that should not be neglected. Namely, the fact that it was very difficult to find an intuitive semantics for some of the membership functions (even though they are producing high quality rules), which complicates the communication with domain experts.We are currently working on this issue and got promising results using heuristics for splitting an merging fuzzy sets.

6. References

[1] K. Franke and S. Srihari, “Computational forensic: An overview,” in Computational Forensics, 2008.

[2] O. Ribaux, A. Girod, S. J. Walsh, P. Margot, S. Mizrahi, and V. Clivaz, “Forensic intelligence

and crime analysis," Law, Probability and Risk,vol. 2, pp. 47– 60, 2003.

[3] C. Bell, "Concepts and possibilities in forensic intelligence," Forensic Sci. Int., vol. 162, pp. 38–43, 2006.

[4] J. McCarthy, "What is artificial intelligence," Stanford University, Tech. Rep., 2007.

[5] A. Engelbrecht, Computational Intelligence: An Introduction. Wiley, 2003.

[6] W. Duch, Challenges for Computational Intelligence. Springer Studies in computational Intelligence, 2007, ch. What is Computational Intelligence and where is it going?, pp. 1 –13.

[7] S. S. Kind, "Crime investigation and the criminal trial: a three chapter paradigm of evidence," J. Forensic Science Society, vol. 34, pp. 155 –164, 1994.

[8] I. Ricci, "Forza - digital forensics investigation framework that incorporate legal issues," Digital Investigation, vol. 3, pp. 29–36, 2006.

[9] A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, pp. 302 – 314, 1997.

[10] I. Evett, L. Foreman, J. Lambert, , and A. Emes, "Using a tree diagram to interpret a mixed dna profile," Journal of Forensic Sciences, vol. 43,pp. 472– 476, 1998.

[11] K. Franke and S. Srihari, "Computational forensics: Towards hybridintelligent crime investigation," in Third International Symposium on Information Assurance and Security, 2007.

[12] O. Ib´a˜nez, O. Cord´on, S. Damas, and J. Santamar´ıa, "Craniofacial superimposition based on genetic algorithms and fuzzy location of cephalometric landmarks," in Hybrid Artificial Intelligence Systems, 2008.

[13] V. Pervouchine and G. Leedham, "Extraction and analysis of forensic document examiner features used for writer identification," Pattern Recognition, vol. 40, pp. 1004–1013, 2007.

[14] M. Girgis, A. Sewisy, and R. Mansour, "A robust method for partial deformed fingerprints verification using genetic algorithm," Expert Systems with Applications, vol. 36, pp. 2008–2016, 2009.

[15] W. Sheng, G. Howells, M. Fairhurst, F. Deravi, and K. Harmer, "Consensus fingerprint matching with genetically optimised approach," Pattern Recognition, vol. 42, pp. 1399–1407, 2009.

[16] J. V. Hansen, P. B. Lowry, R. D. Meservy, and D. McDonald, "Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection," Decision Support Systems, vol. 43, pp. 1362–1374, 2007.

[17] T. H. Grubesic, "On the application of fuzzy clustering for crime hot spot detection," Journal of Quantitative Criminology, vol. 22, pp. 77– 105, 2006.

[18] N. Liao, S. Tian, and T. Wang, "Network forensics based on fuzzy logic

and expert system," Comput. Commun., vol. 32, no. 17, pp. 1881–1892,2009.

[19] C. Quek, K. B. Tan, and V. K. Sagar, "Pseudo-outer product based fuzzy neural network fingerprint verification system," Neural Networks,vol. 14, pp. 305–323, 2001.

[20] P. Castellano and S. Sridharan, "A two stage fuzzy decision classifier for speaker identification," Speech Communication, vol. 18, pp. 139–149, 1996.

[21] S.-T. Li, S.-C. Kuo, and F.-C. Tsai, "An intelligent decision-support model using fsom and rule e xtraction for crime prevention," Expert Systems with Applications, vol. 37, pp. 7108–7119, 2010.

[22] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, pp. 338 –353, 1965.

[23] MatLab R2009a, MATHWORKS, 2009.

[24] E. Klement, R. Mesiar, and E. Pap, Triangular norms. Kluwer, 2000.

[25] R. Yager, "On a general class of fuzzy connectives," Fuzzy Sets and Systems, vol. 4, pp. 235 – 242, 1980.

[26] D. Dubois and H. Prade, Fuzzy Sets and Systems: Theory and Applications. Academic Press, New York, 1980.

[27] M. Sugeno, "Fuzzy measures and fuzzy integrals: a survey," Fuzzy Automata and Decision Processes, pp. 89 – 102, 1977.

[28] L. A. Zadeh, "Outline of a new approach to the analysis of complex systems and decision processes," IEEE Trans. Systems, Man & Cybernetics, vol. 1, pp. 28 – 44, 1973.

[29] S. Fukami, M. Mizumoto, and K. Tanaka, "Some considerations of fuzzy conditional inference," Fuzzy Sets and Systems, vol. 4, pp. 243 – 273, 1980.

[30] E. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," International Journal of Man-Machine Studies,vol. 7, pp. 1 – 13, 1975.

[31] M. Sugeno, Industrial applications of fuzzy control. Elsevier Science, 1985.

[32] J. Dunn, "A fuzzy relative of the isodata process and its use in detecting compact, well separated clusters," Journ. Cybern, vol. 3, pp. 95 – 104, 1974.

[33] J. C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms. Plenum Press, 1981.

[34] L. Li, X. Liu, and M. Xu, "A novel fuzzy clustering based on particle swarm optimization," in First IEEE International Symposium on Information Technologies and Applications in Education, 2007, pp. 88 – 90.

[35] G. Gan, J. Wu, and Z. Yang, "A genetic fuzzy k-modes algorithm for clustering categorical data," Expert Systems with Applications, vol. 36,pp. 1615 – 1620, 2009.

[36] M. P. and P. SK., "Rough set based generalized fuzzy c-means algorithm and quantitative indices," IEEE Trans Syst Man Cybern B Cybern.,vol. 37, pp. 1529 – 1540, 2007