Research Journal of Recent Sciences ISSN 2277-2502
Vol. **3(8),** 103-110, August **(2014)** *Res.J.Recent Sci.*

Digital Forensic Models: A Comparative Study based in large enterprises of Pakistan

Khuram Mushtaque[1], Ahmer Umer[2], Kamran Ahsan[1] and Nadeem Mahmood[3]
[1]Federal Urdu University of Arts, Science and Technology, Karachi, PAKISTAN
[2]Mohammad Ali Jinnah University, Karachi, PAKISTAN
[3]KICT, International Islamic University Malaysia, Jalan Gombak, 53100 Kuala Lumpur, Selangor, MALAYSIA

Available online at: www.isca.in, www.isca.me
Received 29th November 2013, revised 3rd January 2014, accepted 21st February 2014

Abstract

Introduction of Information Technology in the business has not only improved the performance and has opened new doors for the market; contemporarily it has transformed the dependency of large enterprises more towards the efficiency and reliability of this technology. Cyber crime is a type of crime associated with I.T which could not just affect the performance of these organizations but also may ruin their business, reputation and trust in the market. Apart from different security measures to protect these organizations from cyber attacks, Digital forensic is the science which was introduced to find out the culprits once any crime occurs successfully. Digital forensic examiners perform investigation process and collect the evidences which may be admissible in the court of law so that the offender gets penalized and the affected organization restores their financial loss and prevents it to happen again in future. Different modules were introduced since 2001 to 2011 around the globe which divide the digital forensic investigation process into different phases. Because of lack of awareness and slow adopting nature of Pakistan, this science is not being familiarized as much and no any particular module is followed by cyber forensic firms because organizations of Pakistan don't tend to opt for such services with some reservations. In this paper we have identified vulnerable sections in 80 large enterprises of Pakistan in the context of their security measures taken to enable successful digital forensic investigation process. These 80 organizations contained different types of industries, banks, and hospitalsetc where the I.T is used at quite some extent and as reliable tool for their core business.

Keywords: Digital forensic, forensic models, cyber crime, organizational security, forensic investigation.

Introduction

Information technology has become a back bone of most of the large enterprises to not only run their business effectively but also to compete with their competitors in the industry more appropriately. Enterprises in current era are investing immense budget over optimizing the performance of I.T and also improving the security of I.T to protect all the valuable assets and maintain the reputation of the enterprise as well[1]. These organizations are also shifting their business and allowing users to comment or even add comments to their pages[2] environment which provides different new facilities to customer to browse the company and the services they offer by using online search engine[3] and customizations features.

Another highlight able aspect pertaining to this research is that the rapid increase of the usage of different electronic financial and informative transactions by user in order to use the services provided by their banks such as ATM cards, credit cards, debit cards, online utility bill payments, online funds transfers, online balance inquiry and bank statements[4]. All these electronic operations are performed by relying over the security of the concerned organization and other associated companies which are the responsible to provide integrity, confidentiality and availability to the customers[5].

Despite all the essential and possible preventing measures being employed such as usage of Biometrics[6] and other tools to secure and protect the I.T assets, different types of networks including ad-hoc networks[7] and co-related segments, if any cyber crime takes place and has chances of damaging the organization heavily from any dimension, then it is compulsory to acquire the services of digital forensic firms. Allowing access to certain sites like social networking sites[8].

Digital Forensic is known as the process which identifies; preserves, analyzes and presents the digital evidences in such a way which is acceptable legally[9]. It may also include extractions, interpretations and documentations of these computer evidences to incorporate the evidence rules, its legal processes, evidence's integrity, reporting of factual terms of found information and giving the professional opinion in any court of law or possibly for any other legal or administrative proceedings depending upon what was found[10].

The increase in computer associated crimes caused the agencies of law enforcement to startthe establishing of specialized groups, generally at national stage, in order to hold the technical features of investigation[11]. One of first practical which was at least publicized as first cases of digital forensic was the Cliff Stoll's chase of hacker Markus Hess in year 1986. Cliff Stoll,

who analysis made utilization of computer and its network forensic systems, he was not any specialized examiner. Several of the earlier forensic examinations pursued the similar profile[12].

Digital forensics science developed from makeshift tools and practices designed by such hobbyist practitioners during that period. In distinction to rest of the forensics domains it was developed out of work by the community of scientifics[13]. Later on in 1992 the phrase "computer forensics" was utilized in the academic literature; a research paper by Spauland Collier tried to provide justification for this new domain to world of the forensic science. This rapid development concluded in a shortage of training and the standardization[14].

In current research, we selected those types of organizations where I.T is being used by creating more effects over their business and other related operations. It means that if any cyber crime commits in these organizations then it may leave huge impact over their business and may harm their operations as well.

These categories of industries/organizations included banks, software houses, manufacturer industries, hospitals, news/media houses, I.T Integration companies, I.T Vendors, services providers, Telecom industry, Insurance companies, Logistics and few other similar types of organizations where I.T is being used with some extent and its performance is directly associated with their core business and functionalities.

Forensic Models

The forensic process model (2001): It was projected by Ashcroft, U.S National Institute of Justice (NIJ) for investigations of electronic crime scenes which provide a guideline for the very first responders. It is also used by the enforcement andother to protect, recognize, and can of digital evidences. It contains four following phases:

Collection: Here evidences are searches, get collected and felicitated.

Examination: It is to formulate the evidences transparent and get the foundation of its source.

Analysis: It performs the assessment of the result of the phase of examination.

Reporting: It drawsoutcomesand results of all phases and gathered information.

Phase of analysis of current model is inappropriately explained and remains vague.

Abstract digital forensic model (2002): This model was introduced by Carr, Reith and Gunsch. It was based on conventional approach of collection of forensic evidence. This model contains nine following components:

Identification: Helps to recognize and identify the incident type.

Preparation: Preparation of methods, procedures and search warrants.

Approach Strategy: It formulates the processes and approach which will be used in the evidences collection phase.

Preservation: This component used to secure and protecting the available evidences.

Collection: Used to standardize the procedures for physical scene recording.

Examination: Deals with evidences searching of the associated suspect of committed crime.

Analysis: It isthe scrutiny of significance of product that was inspected.

Presentation: It presents the detailed explanation of all involved phases.

Returning Evidence: It is to return the digital sources to the appropriate owner.

Third phase of this model a duplication of second phase to some extent.

The integrated digital investigation process model (IDIP) (2003): IDIP was suggested by Spafford and Carrier. This model converts process of digital investigation into the process of physical investigation process. This model handles the investigation process into five following phases:

Readiness Phase: The objective of readiness phase is to make sure that the actions and infrastructure are capable to provide support to the investigation completely.

Deployment Phase: To supply a system which could detect and confirm an incident.

Physical Crime Scene Investigation Phase: This phase is to gather and examine the physical evidence and rebuild the acts that took place throughout the incident.

Digital Crime Scene Investigation Phase: It is to gather and examine digital evidences those were attained from phase of physical investigation and by some other future way. It contains process same as physical evidence phase; though major focus is to collect digital evidence.

Review Phase: Reviewingtheentireanalysis and highlights the areas of betterment.

The phase of deployment of current model deals with the verification of the incident, but practically it is not possible to certify the digital crime prior toappropriateinvestigation.

Extended model of cyber crime investigation (2004): This model was proposed by Ciardhuain and it emphasizes on the management aspect whereas earlier models were focused only to dispensation of cyber crime evidences in investigation of any cyber crime[15].

Case-relevance information investigation (2005): Gartner and Ruibin, Yun proposed this model. In this model computer intelligence assists in procedures of investigation. Prerequisite of technology of computer intelligence is explained in current model appears as a supporter to procedures of investigation. It is used for description of the amount of case-applicability and also to differentiate between computer security and discipline of forensics.

Digital forensic model based on Malaysian investigation process(2009): This model proposed by Perusal includes the obtaining dynamic and static data. It has been proved that this model is an imperative phase in order to acquire dynamic and static types of data.

The systematic digital forensic investigation model (SRDHM)(2011): This model was Preston, Ademu and Imafidonto assist the forensic examiner andrelevant organization in an appropriate manner. Given under are the Phases of this model:

Phase of Preparation: This phase arises before the real investigation process which engages obtaining preliminary understanding of the type of offense and activities, plan the collected material for packing sources of evidence etc. The analysis must follow the diverse legal limitations and control splusorganizational constraints. This phase also engages getting required search warrants, backup from higher management, necessary authorization and legal notices to all relevantpartiesetcprior to moving towards the scene of crime. A proper policy for inquiry ought to be build up to amplify the class of evidence and lessen the threats.

Phase of Securing the Scene: It mainly deals with safeguarding the scene of crime from being accessed by unauthorized persons and also preserves the evidence from getting infected. Formal protocol must be used to hand over a crime scene to guarantee that chain of custody is followed in a proper manner. Investigators mustrecognizeextent of crime and then set up a boundary. This phase must target the Integrity of evidences. This phase decides the evidence quality; hence it plays a vital role in entire process of investigation.

Phase of Survey and Recognition: Here investigators conduct initial to evaluate the crime scene, identify the probable sources of evidence and formulate a proper plan to search. This might not be so simple in a complex situation. It evaluates the electronic devices found at the scene to decide whether any expert aid is necessary in dealing out the scene. Identification of people in the scene and preliminarily interviewing them are essential. Precious information can be gathered from the users of electronic equipments, owners or from system administrators such as objective of system, schemes of system, different applications used in devices, user names and passwords, details about encryption etc. Investigators should try to plan to analyze the evidences developed after the phase of survey and reorganization.

Phase of Documenting the Scene: Appropriate documentation of the scene where crime committed together with photographs, sketches and mappings are performed in this phase. Visible data must be documented, which assists in recreation of the crime scene and review it any time. It is vital when the forensic specialist has to perform a court testimony, which can be several months past the investigation process. Status around the incident with those who informed about the incident at first and at what time and date must be incorporated as well to maintain a log of those who were there on the crime scene, those who arrived later and those who left the scene etc, together with the outline of their activities during their presence on the scene.

Phase of Communication Shielding: In this phase all additional communication alternatives of the relevant devices must be blocked including Bluetooth and wireless services which could be utilized to overwrite the vital information. Finest option after blocking a device is to segregate it after disabling it'sall communication capabilities.

Phase of Evidence Gathering: Evidence gathering of the digital or mobile devices is a necessary step which requires a suitable system or rule to make them work. It can be further categorized two following categories:

Volatile Evidence Gathering: Most of the evidences which involve mobile devices are volatile type being present in ROM. Gathering volatile type evidences delivers a difficulty as the device condition and content of memory might be modified. Immediate decision making is needed in case of low battery and image creating with swift tools is the top option in such situation with supplying of ample power by doing replacement of batteries or by using other power adopters.

Non-volatile Evidence Gathering: Gathering evidence from external media of storage supported by these devices akin to memory sticks, MMC cards, USB flash drives etc. Computer Evidence those are harmonized with devices should be gathered by utilizingsuitabletools of forensic which is permissible in the court of Law. Authenticity and Integrity of the evidence gathered must be certified by usingtechniquessuch as write protection and hashing. All adopters, power cables, structure and other relevant accessories must also be gathered.

Phase of Preservation: In this phase packaging, transportation and storage are performed to keep important electronic evidences from being modified. All probable sources of evidence must be recognized and tagged correctly. The device and other accessories ought to be placed in an envelope and fastened prior to putting it in evidence bag and restrict all more potential communications with them and required temperature, keeping it away from dust or additional heat are also points that must be considered.

Phase of Examination: Itisexamination of the content of the gathered evidence by forensic experts and taking out the information. Proper quantity of evidence backups should be produced. Its aimis to make the evidence noticeable, whilst defining its integrity and implication. Personal organizer data such as text and voice messages, emails and documents and are few of the familiar evidence sources which will be analyzed fully. Detection and recovery of concealed or masked information is a main boring task involved in this phase.

Phase of Analysis: A technical evaluation performed by team of investigators on foundation of outcomes of the assessment of evidence. Identification of relationships between sections of data, analyzing of the data that is concealed etcare few of the main activities done in this phase. Results of the phase of Analysis might specify the requirement for extra steps in the processes of analysis and extraction. Results of analysis must be documented correctly.

Phase of Presentation: After gathered evidences being extracted and analyzed, obtained results might require to be presented in front of a broad diversity of audience that includes law enforcement officials, legal and technical specialists, corporate management etc. After this phase, it ought to be likely to verify or abandon the accusations concerning the exacting offence or doubtful incident.

Phase of Result and Review: The concluding phase of this model is the phase of result and review. This phase engages reviewing every step in the investigation and recognizing the areas of betterment. The outcomes and their following explanation can be utilized for additional cleansing the collection, assessment and analysis of evidence in the prospect investigations. In numerous cases, a great deal of iteration of assessment and phases of analysis are needed to acquire the whole image of an incident or crime occurred. This obtained information will also assist to create improved policies and procedures in place in future[16].

Discussion

In Pakistan, cyber crime is rising swiftly with the supportive increase in use of cell phones and internet access. It has been also seen that latest technology has been used by criminals in order to accomplish their criminal plans. Such types of criminals are involved in monetary matters, stealing of information and sometimes in terrorism.

If we study the situation of Pakistan comparatively with other advanced countries of the globe, we will come to know that the laws against the cyber crime are not regulated as much as they need to be. More than often the cyber crime is not been taken seriously and the severity of its impact is calculated lesser than it has to be.

The justification of this remark is that despite the internet and other technology indulged in the enterprises level many years ago but the law of accepting the digital evidences in the court of Law is approved in March 2013. It shows the delay in acknowledging the worth and significance of technology in order to control and counter the crimes by using the technology[17].

National Response Center for Cyber Crime (NR3C) is established as the sub-branch of Federal Investigation Agency (FIA) of the Pakistan. NR3C is competent to observe, follow and grab all such criminals. NR3C has provided a single-point of contact for all organizations including local and foreign for all issue associated to cyber crimes in the Pakistan. It is providing training and educating the government or semi government and private sector organizations about the education of security. Number of seminars and workshops are also conducted in different cities of the country to provide sensitive government organization concerning cyber attacks on their critical resources of information, breeches in information and to secure their systems against all such type of cyber threats[18].

There are very few enterprises in Pakistan who acquire the services of Cyber Forensic firms in case of any cyber crime occurrence. The basic reliance they prefer is the Insurance service, since they could easily get the financial loss by using the facility of insurance therefore they don't go for the cyber forensic firms and their services in order to establish culprit and gather its evidences.

There are few reasons behind such attitude of enterprises in Pakistan such as they don't want to further invest over the services of Cyber Forensic firms after facing loss already because of the cyber crime. Another reason is that the organization doesn't want lose their reputation in the market by disclosing their name in the cyber crime affected enterprises because it may establish that they are technologically vulnerable. Another reason is the weak system of court of law as it is extremely stiff to prove anybody culprit in the court by using gathered digital evidences as the court system is not technically sound in this sector and also it is time consuming.

Findings: i. The findings presented in this section are based on the study of large enterprises of Pakistan. ii. In this section, we have raised critical issues in regarding diversified approaches towards adopting the necessary steps in order to control the elements associated with evidence gathering process during digital forensic investigation process. iii. First comparative analysis is between the enterprises of similar types of business with each other and second comparison performed here is

among the organizations of different types with each other comprising IT.

Deviations between different Industries while adopting the necessary steps regarding Digital Forensic

The ratio of those I.T personals that are aware about the domain of cyber forensic, its significance and its pros and cons in the current era is quite diversified and in some sectors quite low as well. Least weak sector in this context is banking while weakest of all is the News/Media industry in Pakistan.

As far as the awareness of digital forensic in their industry is concerned, we found that weakest industry is supposed to be I.T Integration with no any I.T responsible person knowing about digital forensic at all, while Banks with 92% were the least weak among all the industries addressed above.

It has been identified that I.T vendors sector pays slightest importance over incorporating the digital forensic domain in their formal institutional plan with 75% of percentage. On the other hands, 50 % Banks, Hospitals, I.T Integration and Service Providers include it in their formal institutional plan which isn't a big number as well.

It has been seen that No any I.T Integration organization acquire the services of cyber forensic firms, whilst less weaken sector in this segment is I.T vendors because 50% of I.T vendors acquire the services of cyber forensic firms for their organizations.

If we consider the percentage of organizations of different industry types that conduct any awareness training program for employees to educate them about cyber crime and forensics then we find that Telecom sector with 75% of organizations don't follow it is the weakest of all while Banks with just 9% is the least weak of all the industries of Pakistan.

By considering comparison of the probability of occurrence of cyber crimes/incidents in the organizations, we come to know that 67% I.T vendors industry face this issue once in a week. While the strongest of least weaken industry in this perspective was identified manufacturers and telecom industries with 75% each of these organizations go through the situation of cyber crimes/incidents rarely.

I.T Integration industry is the weaken of all with 67% don't employ clause addressing cyber crime in their hiring terms and condition document, on the other hands 100% of the Manufacturers employ it are identified as least weak of all types of industries in Pakistan analyzed in this research.

Our finding demonstrates that 50% of Telecom industry doesn't conduct IT audit function separate from general Audit, which is the most vulnerable sector of this research while the least vulnerable is the Banking of Pakistan sector since 100% banks conducting it.

It has been identified that 100% Telecom and Banking sector addressed in this study don't employ any key strokes typing tools in client computers, which is most vulnerable sector in this context while 75% of hospital industry of Pakistan have installed it is the least vulnerable industry in Pakistan as far as this comparative research is concerned.

100% Hospitals and I.T Vendors sector allow clients to modify date and time of the systems, these both of most vulnerable sectors of Pakistan while least vulnerable sectors identified are Telecom and I.T Integration industries with 100% have restricted clients to modify the date and time of the systems.

Findings show that 75% of I.T Integration industry of Pakistan addressed in this study don't employ any program of screen or real time recording to monitor client computers which is the weakest segment of all the industries while Hospitals and I.T Vendors are the least since 75% of these both industries of Pakistan have installed such programs.

According to our study, Banks are identified as most vulnerable in the context that 67% banks of Pakistan don't use real time monitoring software for client desktops, whilst 100% of Hospitals in Pakistan addressed in this comparative study have employed such programs are identified as least vulnerable in this perspective.

75% I.T vendor organizations don't have adequate number of cameras installed, therefore this industry is weakest while 100% hospitals in Pakistan addressed in this study have installed adequate number of cameras, thus, this industry is the least weak by comparing it others in this context.

In current finding It has been found that I.T Integration and I.T Vendors are the types of industries of Pakistan which are most vulnerable than others discussed in this study in the perspective of storing the recorded videos durations, as 100% of these both industries store these videos less for less than 1 year. Whereas Banks are less vulnerable than all others as 42% of Banks keep store these videos forever.

75% I.T Vendors don't have the policy and procedure for digital record keeping with reference to forensic investigation at any stage of organization life, it is the weaken industry here while less weaken is News/Media with 35% organization follow this basic principle with reference to forensic investigations.

We came to know that most weaken among all is the 83% Manufacturers industry don't have independent audit review procedure for fitness of C.C.T.V cameras before or after the purchase of equipment through forensic Audit firms, while less weaken industry is I.T Integration industry with just 33%.

Statistics of this finding shows that 50% of I.T Vendors and I.T Integration companies don't take the backup of recorded videos captured by C.C.T.V cameras which is the weakest segment of

large enterprise in Pakistan in this perspective while less vulnerable is shown as Software Houses with just 9% of them not following its basic principles of taking video backups.

Hospital, I.T Integration and Telecom sector is the weakest segment of Pakistan's enterprise in the context of using Biometrics system as 50% of all these industries don't use it. Besides it the least weak segment of enterprise in this context is I.T Vendors and Services Providers with just 25% of them not using it.

As far as our findings are concerned, Hospital, Software House sector is the weakest segment of Pakistan's enterprise in the context of using Card Swiping system as 75% of all these industries don't use it all. Moreover the least weak segment of enterprise in this context is Manufacturers with just 17% of them not using Card Swiping System.

We came to know that most weaken among all is the 88% Service Providers industry as they don't have any restriction over using blue-tooth inside the organization, while least weaken industries of Pakistan in this perspective are Hospitals and I.T Vendors with just 25% don't put any restriction over blue-tooth inside the organization.

Discovered by our findings that 42% Software Houses don't have the policy installed regarding the User and Accounts restrictions, therefore, it is the weaken industry here while least weaken are Banks, I.T Vendors, I.T Integration, Manufacturers and Telecom Industries as 100% of them have policy regarding this issue.

It also has been established that 75% I.T Vendors have allowed freeware downloading on computers by employees,
which is most vulnerable industry of Pakistan in this perspective; comparatively banks are least vulnerable against this issue as only 8% of banks in Pakistan have allowed this to happen.

We also came to know that most weaken among all is the 43% Service Providers industry as they don't store the logs of users' activities on server, whilst least exposed industries of Pakistan in this context are Hospitals, I.T Vendors and News/Media with 100% of these organizations store such users' logs on server properly.

Statistics provided in our finding exhibit that 63% of Services Providers don't store application logs and maintain on client, which is truly weakest sector of large enterprise of Pakistan, on other hands less weak industry has been found Manufacturers with just 17% of these types of enterprises don't perform this step of storing and maintaining the logs.

It has been originated that 86 %News/Media industry of Pakistan retain the logs of employees' computer activities for the period of less than 1 year which can be identified most vulnerable than others discussed in this study in the perspective of retaining logs. Least exposed or vulnerable in this perspective is Hospital Industry where 50% of entire industry of Pakistan evaluated I this research retains these logs forever.

Our finding establishes that most weaken among all is the 33% Telecom industry as they don't have a formal intrusion detection program other than basic logging for monitoring host and/or network activity. Minimum weak here we found are the Hospitals and I.T Integration industry where 100% of organizations adopt this mechanism.

It has been recognized that 50% Software Houses have not incorporated procedure and process to record the entry and exit from Datacenter, which is the most vulnerable industry. Mean while Banks, I.T Integration and Hospitals are the least weak in this context as 100% of these organizations have implemented such proper mechanism.

50% Telecom Industry of Pakistan examined in this research don't have any mechanism to record network and systems configurations; it has been established as utmost weak sector. Comparatively 100% Hospitals have adopted such mechanism and was declared as least vulnerable industry in this research.

It establishes that most weaken among all is the 43% News/Media industry where user doesn't get locked after attempting some limited number of wrong passwords being entered. Minimum weak in this perspective are the Banks, I.T Integration and Telecom sector where 100% organizations have applied such restriction.

We found that 100% I.T Vendors allow client computers to save the critical data directly to their own storage media, therefore this industry found most vulnerable in this context. Least vulnerable industries found were 75% of each Hospitals, Services Providers and Telecom organizations in Pakistan.

We find that 67% I.T Integration companies have not implemented policies to prohibit users from allowing anyone
else to use the computer after they've logged in; it has been found as most vulnerable industry in this context. Least vulnerable industry we find here is the Telecom Industry with 100% implementing these policies.

It has been identified that least strong industries in the context of employing snapshot tools to collect evidences and monitor the screens are the 50% Hospitals, I.T Integration and Services Providers each. Least weak industry identified here is the Manufacturers as 83% manufacturers employing snapshot tools.

57% Banks and Services Providers of Pakistan examined in this research have not restricted users to erase the web browser's history and temp files, therefore Banks and Services Providers are the most vulnerable industry of Pakistan in this context.

While least vulnerable is News/Media industry with 86% applying this restriction.

Conclusion

In this paper, we have addressed situation or status of the Digital Forensic in the different types of large enterprises of Pakistan.We highlighted the vulnerable situations could be faced by the organizations to confront against the cyber crime as these organizations are not fully aware about the standard of the security elements need to be focused and organized in the context of the digital forensic investigation model. Since there isn't any uniform standard is being adopted by the enterprises to manage the digital forensic associated security segments therefore it creates a flaw in the entire enterprise world of the Pakistan.

By evaluating the security of same element between 2 or more organizations of same types of businesses we find various deviations between them. On the other hands, by applying same element to different types of organizations also came up with shocking and totally different results with each other in many cases. It is because of no any uniform standard being followed by these enterprises to address the digital forensic investigation domain.

Our research could become an effective guideline for organizations to address these elements at the enterprise level, because we have highlighted all core issues in large enterprises of Pakistan that were identified as vulnerable and need to be addressed. Although the priority and nature of business of these enterprises also may vary, but still, these diversified elements need to stand at single point to mitigate the differences among them.

Our overall research might be effective and prove to be a guideline for many organizations comprising I.T at any level, not to just monitor and manage the cyber crime situations, but also enhance their business, sustain it by initializing the successful accountability mechanism within their organizations and also by enabling the successful process of digital forensic investigation after addressing the vulnerabilities that were raised in this research.

References

1. Muhammad Asif Khan and Hussein Zedan, Alignment Strategies and Frameworks in Co-Evolution of Business and Information Technology, *International Conference on Information, Networking and Automation (ICINA), IEEE,* (**2010**)
2. Mafaza Sajid and Sarah Mansoor, Usability Testing of Wiki's, *Research Journal of Computer and Information Technology Science ISCA,* **1(5),** 1-7 **(2013)**
3. Patil Swati P.1, Pawar B.V.2 and Patil Ajay S., Search Engine Optimization: *A Study, Research Journal of Computer and Information Technology Sciences*, ISCA, **1(1),** 10-13, **(2013)**
4. Abirami Sivaprasad and Smita JangaJe, A Complete Study on Tools and Techniques for Digital Forensic Analysis, *International Conference on Computing, Electronics and Electrical Technologies ICCEET*, *IEEE,* **(2012)**
5. P. Salini and S. Kanmani, A Model based Security Requirements Engineering Framework applied for Online Trading System, *IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, 978-1-4577-0590-8/11/$26.00 ©2011 IEEE, MIT, Anna University, Chennai,* **(2011)**
6. Narmeen Bawany, Rabia Ahmedand Qanita Zakir, Common Biometric Authentication Techniques: Comparative Analysis, Usability and Possible Issues Evaluation, *Research Journal of Computer and Information Technology Science,* **1(4),** 5-14, **(2013)**
7. Lakshmi P.S., Pasha Sajid and Ramana M.V, Security and Energy efficiency in Ad Hoc Networks, *Research Journal of Computer and Information Technology Sciences, ISCA*, **1(1),** 14-17 **(2013)**
8. Social Networking: Its Uses and Abuses, *Research Journal of Computer and Information Technology Sciences*, **1(1),** 14-17 **(2013)**
9. Robert J. Walls, Brian Neil Levine, Marc Liberatoreand Clay Shields, Effective Digital Forensics Research is Investigator-Centric, **(2012)**
10. Slim Rekhis and Noureddine Boudriga, Formal Digital Investigation of Anti-forensic Attacks, *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE,* **(2010)**
11. Peter Stephenson and Richard Walter, Cyber Crime Assessment, *45th Hawaii International Conference on System Sciences, IEEE,* **(2012)**
12. Simson L. Garfinkel, Digital forensics research: The next 10 years, *Digital Forensic Research Workshop, Published by Elsevier Ltd,* **(2010)**
13. Aleksandar Valjarevic and Hein S. Venter, Harmonized Digital Forensic Investigation Process Model, *IEEE,* **(2012)**
14. Kara Nance, Brian Hay and Matt Bishop, Digital Forensics: Defining a Research Agenda, *Proceedings of the 42nd Hawaii International Conference on System Sciences, IEEE*, **(2009)**
15. Ayaz Khan, Uffe Kock Wiil and Nasrullah Memon, Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level, *Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE,* **(2010)**

16. Mr. Ankit Agarwal, Ms Megha Gupta, Mr. Saurabh Gupta and Prof. (Dr.) Subhash Chandra Gupta,Systematic Digital Forensic Investigation Model, *International Journal of Computer Science and Security (IJCSS*), **5(1), (2011)**

17. President signs fair trial act into law, http://pakistantoday.com.pk/2013/02/20/news/national/president-signs-fair-trial-act-into-law/ [Access : 04-02-2013] **(2013)**

18. Cyber Crime Law in Pakistan, http://cyber-crime-law.com/2013/03/17/cyber-crime-law-pakistan/ [Access: 02-10-2013] **(2013)**