Malik *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 2 issue 2 April-June 2018

Effective Prosecution to Support Digital Forensic Evidence during Investigation and Court Proceedings

Aftab Ahmad Malik [1] Engr. Mujtaba Asad [2] Waqar Azeem[3]
Professor Department of Computer Science, Lahore Garrison University (LGU)
Lahore Pakistan[1]
Department of Electronics and Electrical Engineering, Shanghai Jiao Tong University
Shanghai Minhang Campus, China[2]
Senior Lecturer, Department of Computer Science, LGU; Lahore Pakistan[3]
Email: dr_aftab_malik@yahoo.com[1], mujtaba.asad@live.com[2], waqar.azeem@lgu.edu.pk[3]

Abstract:

Firstly, the purpose of this work is to highlight the significance of digital evidence that exists in the form of digital data and is to be presented in court of law. Secondly, how this evidence (the digital information) can be effectively used during investigation process by the investigating agency. Thirdly, essence of keeping up continued liaison by investigating agency with the prosecutor who is to defend the prosecution side in the court. This paper deals with the offences carried out by offenders using computer, internet, digital media, other electronic devices, hacking and tracking the networks to harm the government agencies or private organizations by violating the network or database or cyber security. These offences are normally the frauds related to financial crimes category and illegal transfer of digital currency. Certain crimes of this area are classified as cyber terrorism. The procedure of collection of evidence and presentation in the court is deviant from other criminal cases. The initial digital evidence may consist of data acquisition, databases, data marts, hard disks, computer file systems and records of illegal transfer of money, This paper advocates to employ powerful prosecution in court of law to make the evidence stronger and consistent with the existing law at the investigation stage as well as in court. The focus of this paper is towards banking frauds and cyber crimes requiring forensic evidence to support the task of prosecution.

Keywords: Cyber Crimes, Cyber terrorism, Forensic Evidence, Prosecution.

1. Introduction

This paper deals with offences of criminal and civil nature. With the advent of new techniques of storage and retrieval of information using computer systems, networks, data bases, data marts, data warehouse technology, data mining and cyber space, we need to preserve and use this technology in the area of criminal information systems. According to [1] and [2] in criminal Information Systems, the most important factors to store are Iris code, DNA, face prints

and fingerprints, which are useful to retrieve the records of criminals and part of forensic evidence. The discipline of forensic science [1] helps to get the criminal information hidden in the digital storage devices such as mobile, computers or other electronic media. The information connected with crime or procured from the place of offence can be initially stored then consolidated, interpreted and used as evidence. The rule is raw data is changed into information and the information is converted into knowledge for important decision making or judgments, after proper analysis. For the purpose of analysis of information, one of the tools is provided by biometrics technology [1] for recognition of handwriting, fingerprints, DNA, face prints, criminal images prepared by artists and matters related to encryption and decryption of information, which is to be used as evidence in criminal investigation and court proceedings. Apart from the essence of the evidence to related banks accounts, ledgers, [2] stresses upon using polygraph, DNA, face prints, fingerprints, modus operandi, extracts from databases of criminal as evidence for investigating officer and attorney.

2. Review:

In order to facilitate the presentation of fresh idea presented in this research paper, the following points are required to be reviewed.

2.1 The Modus operandi

It has been emphasized in [2],[3],[4],[5] and [6] to cater a column in criminal database to indicate the modus operandi, which is of great importance. The modus operandi of different criminals may be different but normally a criminal while repeating similar offence adopts previous modus operandi or slightly deviant one. Same trend occurs in groups of criminal.

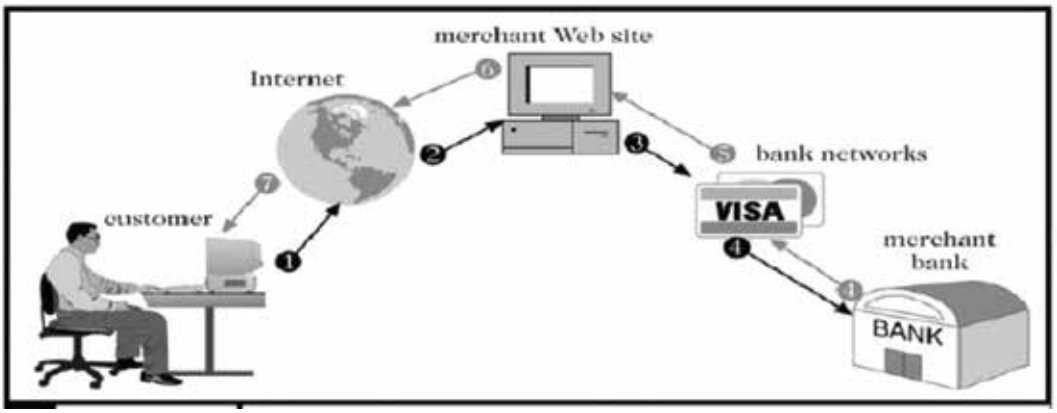
2.2 Financial Frauds and Cyber Crimes

Nowadays most commercial, governmental and private organizations possess computerized management control and information systems for the purpose of storage and information retrieval of their work data. The crimes [2],[3] concerning with using the Computer, internet or electronic Systems connected with Computer networks are categorized as cyber-crimes. The financial frauds are common committed using Cyber facilities by attacking, hacking and tracking into the computer networks systems illegally. There are various ways to commit these frauds such as Email spam, cyberbullying, and committing frauds in on-line business transactions. The security of the computer network systems is of extreme importance and must be maintained at any cost to prevent Data loss, spam emails, hacking and tracking using well known techniques in software and hardware. However [8] proposes to take security measures using firewalls and encryption algorithms.

The purpose of this article is to provide information about cyber security. It gives an analysis that would be useful in taking measure to prevent attacks. The judgment of this analysis is made by expertise and knowledge of databases, hardware, encryption, networks, and firewalls. Moreover it

2.3 Online Payment Systems

Several cyber crimes are committed due to unethical practices during data tractions [9] using online payment systems while customer pays for goods or services. In such systems, we don’t use written checks or cash and transfer the amounts online electronically using methods of mobile and telephone transactions, direct debt from account and electronic money order payment for the billing etc.

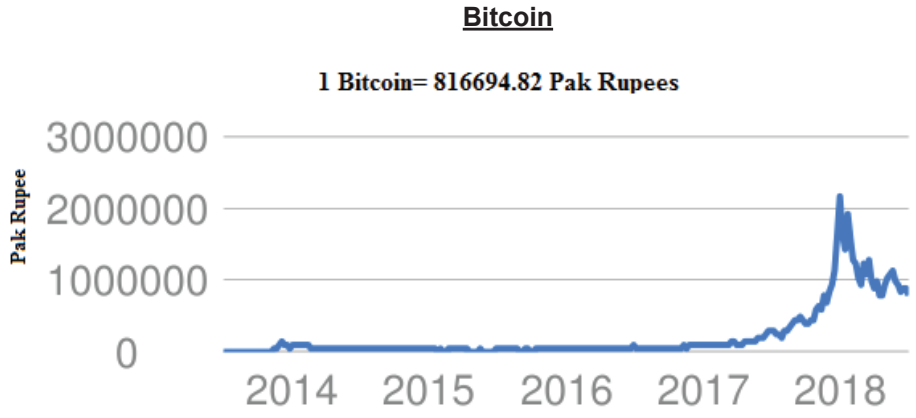


Source: Ritesh Goyal / electronic-payment-system [9]

2.4 Digital Currencies

There exist various digital currencies such as Crypto currency and Bitcoin. The use of the digital currencies has been described by [10] as the online way of transactions by the customer to the merchant for online payment. The digital currencies are called Altcoins. The crypto currency i.e. the Bit coins, Ripple, Litecoin, Tron and Dogecoin etc.

Source: www.moneycontrol.com/cryptocurrency



Source: https://www.coindesk.com/price

2.5 Financial Loss Due to Data Loss

There may be a potential financial loss [11] in using Crypto Currency due to Data loss because it is a virtual currency; therefore, it is inherently risky sometimes. The proposed solution [11] to be on the safe side is to store money in a physical data storage device. There are several offences committed, what is termed as bank fraud. The Central Bank of Pakistan known as State Bank has a supervisory role to play as far as governmental, semi-governmental or private banks are concerned. The State Bank has to implement all rules regulations and monitory, the financial and fiscal policies. The State Bank must take notice where there are irregularities and malpractices occurring in the working of other banks. All government possess inherent trend to help their party members to enjoy undue financial gains through frauds, loans, contracts or illegal allotments. The transactions are to be processed through the commercial banks, therefore, the State Bank under the powers vested, must initiate and take legal action. Most of the times the banks process and deal with false invoices and fictitious/bogus claims of huge amounts. The regime of President Pervaiz Musharraf introduced National Reconciliation Order (NRO) to oversee the malpractices of the past but the Supreme Court of Pakistan declared the NRO to be void and illegal.

3.0 Evidence

According to [2] and [7] the evidence is a fact which can be used in a court to prove another fact. The Law of Evidence, "Qanun-e-Shahadat" was introduced and promulgated in Pakistan in 1984, which defines the categories of evidence such as oral, Circumstantial evidence, Direct, Secondary, Primary or original documentary (public or private). It provides the manner how to present the evidence in the court of law.

3.1 Prevention of Electronic Crimes Act (PECA)

This Act was promulgated in 2016 in Pakistan to prevent offences committed to harm information & cyber systems and to provide legal facilitation and procedure for investigation, prosecution and international cooperation.

4.0 How the Criminals Commit Financial Cyber Frauds?

The financial frauds are committed by causing damage to information system, its access, by changing location, damaging the data virtually using electronic, magnetic, and biometric or any other device. Under the provisions of [12] Prevention of Electronic Crimes Act 2016, the data and passwords are procured by criminals illegally, transaction of data are copied, and interference to data and the information system is caused to commit financial frauds. The damage is also caused by unauthorized interference into one's system or network to alter or spoil the useful information. The offender commits financial forgery or frauds of similar nature of offenses, which have interconnectivity in their approach or modus operandi.

4.1 What Type of Evidence is required by the Prosecutor?

The information gathered during investigation in fraud cases regarding Cyber Crimes must be shared at all stages of investigation and legal opinion of the prosecutor must be obtained. It has been observed that in various court decisions, due to lack of relevant evidence consistent with provisions of law, the courts

have dismissed even the serious cases pertaining to frauds, malpractices, illegal transactions and cyber terrorism. In such cases normally the following type of evidence is essentially required which was used in offence:

- Data on Computer hard disk or CD's or other external cyber media such as internet, intranet or extranet,
- Messages and Emails of criminals,
- Record of Text or voice messages on Mobile,
- Relevant Software to retrieve the information,
- Relevant Record taken from Data Marts, Databases and Data warehouse mined properly,
- Evidence regarding transmission of infrastructure data,
- Data related to on-line-payments
- Credit card No used in fraud,
- Record of Fraud using hacking
- Record of recovered computer files and hard disks ,
- Record of Emails relevant to fraud
- Relevant Image files,
- Procuring complete Transaction Record.

Some of the offences where the above mentioned evidence is essentially required by the prosecutor are computer & internet frauds, frauds using credit card information illegally, counterfeiting, undue financial gains, embezzlements, frauds & thefts in the financial institutions and trading etc.

It is not the responsibility of the prosecutor to investigate guilt and blame of offenders, but the investigating officer is responsible for collection of complete evidence along with the conclusion of the investigation. However, cooperation and cohesion between the investigating agency and the Prosecution is a key to success in court. The defense lawyer can firmly fight out the case, if and only if he is equipped with all necessary information mentioned above. The expert prosecutors having experience in modern technology and law must be engaged who can deliberate on physical exhibits of the case effectively.

4.2 Legally admissible documents be arranged in groups

The subject of legitimacy of evidence is of high significance. There may be hundreds or thousands of documents which are to be exhibited with court file as evidence. This proposes that all the exhibits must be logically arranged into smaller groups keeping in view that how the prosecutor is to defend the case in court. The most irrelevant and legally invalid or inadmissible evidence may either discarded or kept separately for verbal deliberations, if and only if really needed to connect the sequence of fraud or offence. Under the provisions of the the Law of Evidence, "Qanun-e-Shahadat" or Prevention of Electronic Crimes Act (PECA)[13] or any other law, the evidence which is legally admissible can be tendered in the court.

5. Recommendations:

- The prosecutors and investigators must be well conversant with nature and objectives of their profession and gain

adequate proficiency in skills, in the areas of financial accounting investigation and techniques and matters related to conveyancing and pleading in the court of law.

- The investigating agencies and NAB must vigilantly search and investigate where frauds occur or is reported.
- High light criminal schemes of frauds and take cognizance with help of capable and honest investigators,
- Law enforcement must be mandatory for all people specially the influential and high ups,
- The periodic training of the investigators and prosecutors must be made mandatory to improve legal knowledge, investigation skills and norms of court practice,
- The knowledge and skills of investigators and prosecutors must be improved in the area of Computer Science, Information Technology, Software Engineering, Forensic Science, Banking, Law and commerce by introducing short courses in a university.
- The State Bank should not hesitate, because it is duty bound to report all the cases falling within the jurisdiction of National Accountability Bureau (NAB). The cases to be reported on top priority relate to audit reports, bad loans, loans rescheduled and losses caused to the national exchequer by malafide and frauds.
- The State Bank must ensure the implementation of code of business ethics in Banking Sector [14].

6. Conclusion:

The digital and forensics evidence is high significance which must be presented in court of law tactfully, effectively and arranged in logical sequence. The cohesion between investigating agencies and prosecutor must be considered as a strong strategy in cyber frauds and banking sector. Norms of business ethics must be implemented in financial organization in all tiers.

7. Acknowledgement

All the authors are grateful for the appreciation of our work presented in this paper by Mr Kaukab Zuberi Director DFRSC, Lahore Garrison University Lahore.

8. References:

[1] Aftab Ahmad Malik, Mujtaba Asad, WaqarAzeem (2017), “Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed” ; IJECI :International Journal of Electronic Crime Investigation; Volume 1, Issue 1, October-December 2017 Pages 1-10, Lahore Garrison University Lahore.

[2] Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem, DNA Fingerprints Facial Prints And Other Digital Forensics As Evidence In Criminal Investigation and Court Proceedings” ; Volume 2, Issue 1, January-March 2018; Pages 1-10, Pages 1-9; Lahore Garrison University Lahore.

[3] Aftab Ahmad Malik: “Algorithm for

Coding Person's Names in large Databases/ Data Warehouses to enhance Processing speed, Efficiency and to reduce Storage Requirements"; Journal of Computer Science and Information Tech- nology, LGURJCSIT, Volume 1 issue 1, January-March 2017; ISSN 2519-7991

[4] Aftab Ahmad Malik & Asad Mujtaba: "Algorithm for using Codes in place of Facial images during Image Processing in large Databases/ Data Warehouses to reduce storage, Enhance efficiency and Processing speed; Journal of Computer Science and Information Technology, LGURJCSIT, Volume 1 issue 2, April-June 2017;pp 1-9; ISSN 2519-7991

[5] Aftab Ahmad Malik: "Software for Finger Prints Storage and Retrieval of Criminal Identification System for Police", Research Journal, University of Engineering Technology, Lahore, Volume 12; No. 4; PP: 1-18

[6] Aftab Ahmad Malik: Software for Storage and Retrieval of Criminal Information for Police", Research Journal, University of Engineering echnology, Lahore, Volume 13; No.1 PP: 1-28

[7] John William Salmond, " Jurisprudence" , Ebook: ww.ebooksread.com/authors-eng/john-william-salmond/jurisprudence-mla shtml

[8] Syeda Marrium Nizami and Gulfraz Naqvi, " The Reality of Cyber Security ", Vol.1 issue1 Oct-Dec 2017, Lahore Garrison University

[9] Online payment system, https://securionpay.com/blog/e-payment system

[10] Online payment system, https://www.slideshare.net/RiteshGoyal/electronic-payment-system

[11] Mohsin Ali (2017), "Crypto Currency in Cyber world ",; IJECI : International Journal of Electronic Crime Investigation; Volume 1, Issue 1, October-December 2017, Vol.1 issue1 Oct-Dec 2017, Lahore Garrison University, Lahore.

[12] Brian Martucci (2018),"What Is Cryptocurrency–How It Works, History & Bitcoin Alternatives", Posted in: Banking Economic Policy, Money Crash, June 2018; https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

[13] Prevention of Electronic Crimes Act (PECA)

[14] Aftab Ahmad Malik (1995), "Business Ethics in Banking Sector", Book Published by Institute of Banking Sector, Karachi.