P-ISSN 2708-6453	Pakistan Languages and Humanities Review	January-March 2025, Vol. 9, No. 1
O-ISSN 2708-6461	https://doi.org/10.47205/plhr.2025(9-I)55	[617-627]

Pakistan Languages and Humanities Review
www.plhr.org.pk

RESEARCH PAPER

Digital Forensic and the Investigative Structure of Pakistan: An Assessment

[1]Qurrahtulain , [2]Dr. Sardar M.A. Waqar Khan Arif and [3]Bushra Bannian

1. Assistant Professor, Department of Public Administration, Faculty of Management Sciences, University of Kotli, Azad Jammu and Kashmir, Pakistan
2. Assistant Professor of Law, Department of Law, Faculty of Social Sciences and Humanities, University of Kotli, Azad Jammu and Kashmir, Pakistan
3. Lecturer of Law, Department of Law, Faculty of Social Sciences and Humanities, University of Kotli, Azad Jammu and Kashmir, Pakistan

*Corresponding Author	Qurratulainkhan85@hotmail.com

ABSTRACT

This paper focuses on digital forensic within the context of investigative structure of Pakistan. Digital forensic refers to the methodical recovery, storage, analysis and presentation of digital information. It is a branch of the forensic sciences that deals with the analysis of digital evidence from digital sources Digital evidence is simply a product of a digital forensic process. Unlike traditional forensic sciences, a digital forensic analysis attempts to analyses non-physical evidence, or evidence that cannot be directly observed by humans without the use of forensic examination or interpretation. It is because digital evidence cannot be directly observed that the admissibility of such evidence in court is under constant scrutiny (Antavi, 2021). In Pakistan various devices are used to collect evidence. In this context, this paper analyses relevant laws pertaining to digital forensic within the investigative structure of Pakistan. It analyses relevant laws and discusses its implications in practical terms.

KEYWORDS Digital Forensic, Evidence: Investigation, Inquiry, Pakistani Laws

Introduction

This article focuses on digital forensic and investigative structure of Pakistan. As the evidence is pivotal in civil and criminal proceedings. Digital trade and cross-border data flows can support Pakistan's growth by tapping into the potential of the digital economy. With a national strategy targeted at lifting restrictions on digital trade, Pakistan has the potential to increase its exports, especially in high value-added and content-intensive activities, and therefore reap the benefits of the digital economy. In this context, this revised work on digital forensic and investigative structure analyses the relevant legislation in Pakistan.

Literature Review

Legal Framework dealing with the Investigative Structure of Pakistan

There are two types of laws in the criminal justice system of Pakistan one is substantive laws that describe the offences like Pakistan Penal Code (PPC) and other are procedural in nature like Criminal Procedure Code (Cr.Pc). As the question of investigation of offence arise, the mainframe is given under CrPc, Police is the investigative authority in Pakistan, though the special departments are established under special laws to deal with the special issues, like National Accountability Bureau (NAB) is established

under NAB Ordinance, 1999 to investigate the offence of corruption and to maintain the environment of accountability. To inquire and investigate the matter concerning with Federal Government wests with FIA (FIA Act, 1974). The Code of Criminal Procedure, 1898 is the main law from which the roots of investigation started. It gave whole authority to Police to investigate the matter and to propose a report. The whole procedure is given in Chapter-XIV (CrPC, 1898).

Federal Investigation Agency Act, 1974

Federal Investigation Agency (FIA) is established under Federal Investigation Act, 1974. It is expedient from the preamble of the said Act that the agency is constituted for investigation of offences connected in connection with the matters concerning the Federal Government, the Agency is established under Section 3 of the said Act. The supervision of the agency vests with the Federal Government while the Director General administer the agency. The Act provides proper hierarchy of the officials working on the said platform.

National Response Center for Cybercrimes

National Response Centre for Cyber Crime (NR3C) - FIA is a law enforcement agency dedicated to fight cybercrime. Inception of this Hi-Tech Crime-Fighting Unit emerged in 2007 to recognize and control technological abuse in society. NR3C, is the latest introduction to directive of the FIA, mainly to deal with technology based crimes in Pakistan. It is the only Unit of its kind in the country and in addition to the directly received complaints also assists other law enforcement agencies in their own cases.

NR3C has expertise in Digital Forensics, Technical Investigation, Information System Security Audits, Penetration Testing and Trainings. The Unit since its inception has been involved in capacity building of the officers of Police, Intelligence, Judiciary, Prosecutors and other Govt. organizations. NR3C has also conducted a large number of seminars, workshops and training/awareness programs for the academia, print/electronic media and lawyers. Cyber Scouts is the latest initiative of NR3C, in which, selected students of different private/public schools are trained to deal with computer emergencies and spreading awareness amongst their fellow students, teachers and parents.

The Services offered and rendered by the said Unite includes computer forensic, mobile/cell phone forensic, video forensic, network forensic and technical training. It is evident from the mission and vision statement of the Unit that it combats cybercrimes, provides state of the art digital forensic service, enjoyed its ultimate high and respect among the public due to thorough professionalism, integrity, competence, impartial attitude and service that stays as role model for the provincial police and other law enforcement agencies. The fields in which the Unit is providing thorough service includes hacking, child pornography, data theft, identity theft, cyber Bullying, financial fraud, computer virus and worms, malicious software, intellectual property rights, money laundering, digital piracy, electronic terrorism and extortion etc. the track record of the unit is phenomenal, the main and prime reason behind it is professional, skill and transparency in the management.

Electronic Transaction Ordinance and Digital Investigation

As far as the body of this legislation is concerned, the ETO is multidimensional legislation, it means it has seven directions as it has seven chapters. Its first dimension is to define the terms. The preamble is very much clear about the essence of its promulgation and need no explanation as the same is self-explanatory. The section 2 of ETO, 2002 is a

brief account of the definition of several terms that have been used in the promulgation like "access to data, information, authentication, code, court, data, device, damage etc. the purpose of the definition clause is to define the spirit of legislation.

Chapter II of ETO (offences and punishments) comprises of 23 sections, all of the sections highlighted the offences in the respective field and described the punishments available in this Ordinance. By deeply studying the chapter one should realize that the offences that are endorsed and the punishments that are available are complementing the conventions of the UN. The promulgation in one side describes the offences related to the field but also provided the means to deal with electronic evidence. The chapter is unique and contribute more to embellishment of the whole Ordinance.

Chapter 5 is the most important chapter and is initiated with the establishment of Certification council which is constituted by the Federal Government within 60 days of the promulgation of this Ordinance. It shall be a body corporate having common seal and perpetual succession, having five members, appointed by the Federal Government. The qualification of the members are also provided in the promulgation in hand, one member shall be telecommunications engineer with at least seven years work experience, of which at least one year is in the field of cryptography services. Two members shall be professional or academics with at least seven years work experience in the field of information technology. One member shall have an administrative background with at least seven years' experience in a private or public organization; and one member shall be an advocate with at least seven years' experience and adequate knowledge of laws relating to information technology and telecommunication (ETO, s 19(b).

Section 21 provides the functions of certification council grant and renew accreditation certificates to certification service providers, their cryptography services and security procedures (ETO, s 21 (2) (a). It shall monitor and ensure compliance by accredited certification service providers with the terms of their accreditation and revoke or suspend accreditation in the manner and on the grounds as may be specified in regulations. It shall monitor compliance of accredited certification service providers with the provisions of this Ordinance. It shall establish and manage the repository. It shall carry out research and studies in relation to cryptography services and to obtain public opinion in connection therewith. it shall recognize or accredit foreign certification service providers, encourage uniformity of standards and practices, give advice to any person in relation to any matter covered under this Ordinance and make recommendations to an appropriate authority in relation to the matters covered under this Ordinance the ETO revolves around the abovementioned council, its powers authorities etc. the functionary of ETO is the certification council.

Investigation for Fair Trial Act, 2013 and Digital Evidence

After the promulgation of ETO Ordinance, 2002 the most important document in shape of Legislation is Investigation for Fair Trial Act, 2013. Its objectivity is eminent from its preamble 'an Act for investigation for collection of evidence by means of modern technologies and devices to prevent and effectively deal with scheduled offences and to regulate the power of law enforcement and intelligence agencies and for matters connected therewith or ancillary thereto." The process begins with information to Station House Officer, hereinafter called SHO and ended up to the report proposed by police after completion of investigation.

The Investigation for Fair Trial Act, 2013 in simple words is the extension of Article 10(A) of the Constitution of Islamic republic of Pakistan, 1973, that provides a clear stance

about the "right to fair trial" and in absence of fair investigation, it is not possible to provide this fundamental right to the citizens. The application of this act is so obvious, it is applied inside Pakistan, in the board or aircraft and applied outside Pakistan, on all communications and transaction made in Pakistan or elsewhere on all person, whether the citizens or non-citizens involved in that communication or transaction (Fair Trial Act, 2013).

The bodies that are given the authorities under this law are Inter-service Intelligence (ISI), Intelligence Bureau (IB) and Police. The issue of warrant for search, its execution, criteria for execution, consideration for issuance of warrant is well addressed, if one summaries the act in few words, they may be, the Act revolves around the warrant and its execution by using the scientific digital devices in investigation of offences that may committed within or outside one's country.

Salient Features of Investigation for Fair Trial Act, 2013

The Act is complementary to the Constitutional part that provides the man, a right to fair trial. As the offence is now a days modified and digitalized, the techniques and means of investigation are not computable so the Parliament of Pakistan made some important amendments in the QSO, 1984 and passed some important laws like ETO, 2002, Investigation for fair trial Ac, 2013, Investigation for fair trial rules, 2013 and so on. As far as the main provisions and distinctive features of the Act under consideration is consideration is concerned, it comprises of 39 sections, eight chapters and IV schedules. Chapter 1 is the definition clause that entails and enlightened the primary terms, there are some special terms, like authorized official that hereby means the person not below the rank of Basic Pay Scale-20 (BPS) who represent the applicant on any forum, in a lighter view, he is the representative of the applicant that hereby means the combination of ISI, IB and police.

The functional chapter in the concerned Act is Chapter-2 that provides proper mechanism of application for warrants. The application of this Act is initiated with an application for warrant, before the presentation of application the notification is issued from the applicant towards the authorized officer and he shall prove the reason of the warrant before the minister in order to get permission for presentation of application for warrant. The detailed procedure is being provided on the application to judge for issuance of warrant. The specialty of this proceeding is that the authorized officer needs to justify for what he is in need of warrant, in light of the report that he proposed before institution of application that accompanied with an affidavit about the veracity of the contents of report.

Another specialty of this Act is that, it provides a detail account of the procedure adopted after presentation of application before the court competent to issue warrants. The duty of the judge here is to hear the application of authorized officer within his chamber and pass the appropriate orders, if he issues the warrant he should state the objective of the warrant, and the same cannot be used in any other purpose. The Act also provides the post execution procedure, it hereby means when after execution of warrant, the information and the material gathered if evident, than the authorized officer give an application for registration of case to police and handed over all the material in any shape to the investigator of Police by following the procedure available in the Act (Fair Trial Act, 2013). One most important salient feature of the Act is that the warrant issued under this law could be served outside the territorial jurisdiction of Pakistan through mutual legal assistance either directly or indirectly and the warrants received from outside Pakistan can be executed inside the Pakistan through proper channel.

Investigation for Fair Trial Rules, 2013

These rules are made by the Federal Government of Pakistan, a competent and empowered authority to do so, to complement the preceding law that is Investigation for fair trial Act, 2013. In these rules certain terms are endorsed like person, supporting material and material is being defined with a versed and elaborative idea. As the contents of Investigation for fair trial Act, 2003 enlightened the warrant, its forms, its execution authority, medium of execution etc., the rules thereof described the contents of the report formulated by the authorized officer on behalf of the minister and authority. It briefly enlightens the contents of the report, its mechanism of preparation and preparation before the authority.

The provisions regarding the procedure of production of report, material before the judge are same as available in the main Act, the procedure adopted for registration of case against whom the material is evident or proved. The procedural provisions available in the main Act resembles with the provision available in its extension law, in short words the investigation for fair trial Rules, 2013 are the extension of the Investigation for fair trial Act, 2013 and complement it from the four corners.

The Prevention of Electronic Crimes Act, 2016 and Digital Investigation

The prevention of Electronic Crimes Act, 2016 is also an important promulgation to quote here. It is evident from the preamble of this Ordinance that, this Ordinance is promulgated to save the confidentiality of digital/electronic evidence, and save it from any sort of harm, legitimize the electronic system its integrity and availability and to provide a mechanism for investigation, prosecution and trial of offences to penalize their offenders. By comparing the commencement and area of jurisdiction of ETO, 2002 and Prevention of Electronic Act, one came to know that this enactment have extra territorial jurisdiction, it covers the act committed beyond Pakistan and brought outcomes in Pakistan.

The Act provides a diversity of definition like "electronic" the term electronic includes but not limited to electrical, electronic, digital, and analogue etc., it means the Ordinance have the capacity to give place to any other form which is yet not been identified. As far as the process of investigation is concerned, Chapter IV enlighten the investigation agency, authorize to deal with the investigation of the offence committed under this Act and the Prosecution agency. The authority to investigate the matter shall be constituted by the Federal Government. As for as the process of investigation is concerned the law enforcement authority or the authorized official shall follow the investigation mechanism provided there in the Cr.PC unless contrary to the provision of this Act.

Chapter V of the Ordinance is also an important Chapter, that deals with international cooperation, here it means the agencies of Pakistan aid and assist the international investigation agencies like INTERPOL and the same cooperation is deserved to be returned to Pakistani agencies when they are in need.

Rest of remaining provisions of this ordinance ensure that the right to fair trial can be placed at peak, no section as well as authority act in a manner that violate ones right to fair trial, each provision of this Ordinance complemented the Right to fair trial which is being given by constitution of Pakistan as fundamental right of the citizens of Pakistan. It is pertinent to mention here that the agency or person authorized by the Federal Government or Provincial Government, conduct the investigation on their behalf.

United Kingdom laws dealing with digital investigation

In United Kingdom (UK) the main law that describes the powers and duties of the Police is "Police and Criminal Evidence Act, 1984" it also provides the criminal evidence, police discipline and complain against the police. As far the authority to whom the power of investigation is conferred is concerned the police is the sole investigation authority, in all case the police investigates. The police can collect and process any evidence which is available in electronic from, it is available there where it can be taken away and which has been obtained in consequence of the commission of an offence and it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed. The powers conferred by this section are in addition to any power otherwise conferred. No power of seizure conferred on a police constable under any enactment is to be taken to authorise the seizure of an item which the constable exercising the power has reasonable grounds for believing to be subject to legal privilege.

Another legislation which is very important is the enactment of Computer misuse Act, 1990, it is evident from the preamble that the essence of this enactment is to save the computer from unauthorised access and modification and matters connected therewith. No special criteria is provided for the investigation is provided the Act solely focused on the offences related to computer like unauthorised use.

As far as the process of forensic in UK is concerned UK government created the role of "Forensic Science Regulator" in 2007. The introduction of a regulator was intended to establish quality standards for all forensic service providers in the UK, create a level playing field in the forensic services market, and grant assurances that all providers were producing reliable and robust scientific evidence. A decade on, there remain questions over the effectiveness of this model of forensic regulation. Although there has been significant progress with initial aims and objectives and broad stakeholder engagement, the Forensic Science Regulator still lacks meaningful powers, and significant gaps in regulation remain. Accreditation is not only inconsistent but may be superficial. The Forensic Science Regulator faces serious resource restrictions with debilitating limitations on the Regulator's capacities, while wider austerity measures throughout the criminal justice system hamper efforts to raise standards in forensic science.

Material and Methods

The methodology adopted in this work is qualitative and descriptive. This methodology outlines the structured approach, tools, and techniques that will be used to implement the relevant legislation on Digital Forensic and investigative structure in Pakistan. It follows a multi-stage, doctrinal and evidence-based, approach that combines pedagogical innovation, technological deployment, capacity-building, and continuous evaluation on this topic.

Results and Discussion

Procedure and Application in Pakistan: The Police and other Investigative Agencies

The police, after commission of offence and after lodging of FIR, starts investigation. The Investigating agency collects the evidence from every possible mean. Cybercrime unlike other offence is technical and complicated, it can be executed by person living far away from the place of commission (occurrence), when a person knows about the cyber-attack he is duty bound under the law to disclose in Toto the information before the law enforcement agencies as soon as possible, without disturbing the crime scene even

a minor mistake will destroy the whole crime-scene because the evidence that is under consideration is fragile among all (Antawi-Boasiako, 2017). The specialist of the police gather the possible evidence and footprints of the expected evidence, the investigator during the course of investigation used several techniques and tools because the evidence that needs to be collected is not in substantive and tangible form, there are thousands of digital devices that have been used to collect the digital evidence because the cybercrime is also committed by using different scientific means, techniques and devices. Here the concept of Forensic Readiness (Rowlingson, 2010), given by Robert Rowlingson is very much effective. The process of forensic started after commission of offence, according to Robert Rowlingson the law enforcement agencies like police pre-empt the crime scene by gathering the evidence from the place, the investigation not only benefit the prosecutor in presenting the case before the court but also minimizing the risk. This is basically a post event activity, made by the law enforcement agencies after gathering the enough information about the offence that is being committed. He has given the minimum criteria for the investigation of digital offence, according to him the law enforcement agencies or departments must take part in the investigation of digital offence. This argument of him indicates that how much sensitive, the investigation of digital offence is in actual. The first responder's guide proposed by the US Department of Justice (USDOJ) is also enlighten some features of forensic readiness. According to it the first responder may be;

- Anyone can cop the place of occurrence that contains the evidence in digital format;
- Anyone may process the place of occurrence by cording-off the place and proceed ahead;
- Anyone can make supervision of such process or beginning of digital investigation; and
- Anyone do manage the investigation of digital offence.

No scanty procedure is given by the said department, it just emphasized on teamwork, it highlighted that every member of the law enforcement is responsible for a fair investigation, everyone would be ready at any time to face the challenges, everyone would be ready to face, conduct and managed the digital investigation.

Commission of offence/information/ lodging of FIR

The first step involved in the digital or formal investigation is the information about the commission of offence. The police or any law enforcement authority authorized to collect any process the information of offence. After registration of First Information Report (FIR), an investigation officer is appointed by Station House Officer (SHO) to conduct the investigation. The digital investigation begins with locating the crime scene and cordon-off the same by using the scientific methodology, tools, techniques, skill, expertise and knowledge. The offences related to digital investigation are describes in several Acts like Counter Terrorism Act, 1997, The Prevention of Electronic Crimes Act, 2016 etc.

After the above process the investigator indulge himself in finding the nature of offence, the hidden files and footprints of the offence. This step can only be initiated by a person having the knowledge of IT and law. The investigator may seize all the available articles available on the crime scene like computer, mobile, pan derive, flash-drive, cards etc. The language of the computer is different from the language of other evidences like every information available or used by the computer is in binary form, a number system based only on numerals 0 and 1. Every evidence that is available on the soft or binary form must be copied on several sources to save it from further manipulation.

There may be three dimensions to which the investigator move; one is to collect the substantive pieces of evidence from the crime-seen, here the substantive evidence may include the computer itself, the connecting parts of the computer like hard-disk and motherboard and any other digital device present there in the crime-seen, here the devices may include the mobile phone, the internet source/ Wi-Fi device, pan derive, memory cards, automated cards etc. The second dimension is to collect what is present there in the seized devices, this step is the actual start of digital investigation. In this stage the investigator tries to extract the whole data that is available in the devices or computer that are seized in the first step. By this collection, the investigator establishes a story and connects the facts on the basis of the material extracted.

The investigation enter into the real phase when the investigator collect the information/data available in the compute and other devices, as it is obvious that the data could not be collected by using casual means, because the data available in the computer or any digital device is in the form of electronic record or electromagnetic record (related to or produced by electromagnetism) that could not be collected without digital equipment. The authority regarding issuance of search warrants and search is enlightened in CrPc, the powers and procedure adopted by police in digital investigation stems from CrPc.

As Code of Criminal Procedure, 1898 is the main criminal procedural law which prescribe the powers and authorities of the criminal courts and investigative entities, but in order to shift the burden from police and to refine and specialize the procedure for special crimes, there several laws are passed by which several forces are established, Federal Investigation Authority is one of the example of special investigative authority, established to conduct investigation in special offences.

Federal Investigation agency is established under FIA Act, 1974. It is evident from the preamble of the said Act, it is established for inquiry and investigation of certain offences committed in connecting with the matters concerning the Federal Government. The list of certain offences from PPC is made and the investigation authority has given to FIA after enactment of the said Act. The Police Order, 2002 is the main Promulgation on the constitution of Police and to reconstruct and regulate the police. The order is enriched with the power, authorities and responsibilities of Police in general. As FIA was established for a special task, the Police Order also provided the division and subdivision of police, classification of police for special tasks. The utility of the computer forensic enhanced from time to time due to its accuracy and authenticity initially it was just limited to crime and its investigation but due to modernity and globalization, its utility enhanced with a record, the recent and prominent utilities are in criminal law, corporate law and civil law.

The importance and use of digital evidence and digital investigation in different fields indicates its usefulness in the modern world, the law enforcement agencies used the digital investigation and digital evidence in almost every field, despite the fact, and it was used in the criminal field in the last decades. The utility of digital evidence and digital investigation is increased in the corporate, banking, commercial and civil sector, as compared to criminal field. After seizure of the devices and computers available in the crime-seen the law enforcement agencies/ investigator shifts to the next step that is retrieve the data from the available devices. Data retrieving is of two kinds, one is to collect the files available in the computer and the second is to retrieve (to find and get the information from the computer or to get back again) the missing or deleted files.

The procedure to collect the digital evidence is so sensitive, even a minor mistake will result in empty hands, the evidence that is collected during the course of digital

investigation must follow the basic mandatory requirements, there may be three to four requirements, that must be complemented; the evidence must be collected, processed and used in a normal manner in the environment which is feasible for the such evidence, it must not be contrary to the best rule of evidence, the "the rule of best evidence" means that the collected evidence need no evidence for corroboration, the evidence itself must be the best evidence among all.

The importance of digital evidence and its appreciation before the court of law is dependent on the procedure that is adopted in the collection of evidence, procedure matters a lot in digital investigation just like the investigation of other offences. As far as the crime-scene of digital/cybercrime is concerned, the place is to be seized and saved just like other casual crime-scene, if the same could not be maintained due to any reason it may question the whole crime and its investigation. By perusing the legislation and procedural practices of the world, it appeared to the researcher that there are near four to five steps by which the investigator could save the crime-scene in shape of collected evidence, which in future would be appreciated and admissible before the court of law, on presentation. The prime step is to save and seize the whole crime-scene as it was, after the commission of offence, after that investigator collect the evidence whatever available in substantive or in soft form without any alteration, after that the investigator needs to copy, make the files replicated to authenticate the same, ensuring that the original file is saved from all kinds of risks, data must be collected by using the digital technology, digital tools are to be utilized to collect the evidence and digital evidence must be stored in the digital evidence envelopes separately. As far as the methods of digital investigations are concerned, there are some defined methods that are to be adopted in the investigation of digital offence. These methods are mandatory to be followed because the evidence, that is to be dealt, is the most fragile kind among all and even a minor touch or click may result in vanishing the whole prosecution case, the steps and the true manner of digital investigation/ computer forensic are as follow;

Collection of Evidence

The evidence from the crime-scene in either form should be collected by following the abovementioned guidelines, in order to build the prosecution on the basis that could not be questioned on any forum.

Preservation of Evidence

Preservation refers to "to save the collected evidence" here it means that the investigator must preserve the evidence that he has collected during the course of investigation, there are lot of techniques, tools and methods that are available and legitimized by the laws of different states that are using in preservation of digital evidence, it may be another computer, hard-disk, pan-derive etc. The investigator must satisfy himself on every question and ambiguity, like the source of crime, reasons of crime, involvement of person/persons in the crime and its reason, reason of cyber-attack etc.

Examination of evidence

Examination of evidence means to examine the collected evidence, to determine its authenticity and veracity, this step may include the process of retrieval of missing and deleted files to complement and complete the story of the crime. Whenever the evidence is collected, preserved and retrieved the most important step "analyses" begin".

Analysis of Evidence:

Analysis is the most important stage that begins after retrieval of the data or information, the analyses predict the results of trial of the offence, it includes the computer involved in crime and devices used to collect the evidence, any other relevant data or information that is priority collected by the investigator, established the link between the crime and evidence and it indicates, which data could be hide and which could be opened. After the stage of analyses the investigator could easily predict either the offender is going to be punished or acquitted.

Presentation of Data

Presentation means that data that is analyzed is presented before the court of law as evidence, the ultimate outcome of the above processes is presentation because the whole game is played to present whatever collected, preserved, processed, retrieved and analyzed, before the court of law, having jurisdiction to entertain the same, to decide the matter, considering the same as authenticated and admissible piece of evidence. In short the purpose digital forensic or digital investigation is nothing, but to shape the evidence, in form, that is admissible before the court of law.

Conclusions

The digital evidence is having fundamental value in the criminal as well as civil justice system of the world, the difference found in defining the terms and formulating the procedure through which the successful investigation and forensic examination would be conducted. Pakistan also tried to legislate the laws to counter the expected imminent treats to the current justice system and legislated certain laws on the subject and made necessary amends in the existing laws to make them computable and endorsed the Information Technology in the laws. Important legislation among all is the promulgation of ETO, 2002, the prevention of electronic Crimes Act, 2016, The Investigation for fair trial Act, 2016, the Counter Terrorism Act, 1997, The FIA Act, 1974, Punjab forensic science Agency Act, 2007 etc. are remarkable legislation and continuously giving the results. However, further reforms are needed to resolve issues pertaining to right to privacy and cybersecurity. The patterns of forensic used in developed countries may be used to handle the situation.

References

Antavi, A. (2021). 'a model for digital evidence admissibility assessment' digital forensic. <https://scinapse.io/papers/2751082626>

Anti-Terrorism Act, (1997). s 2 z

Antawi-Boasiako, A. (2017). 'A model for digital evidence admissibility assessment'. Vol 511 IPIF International Conference on Digital forensic

Computer Misuse Act, (1990). Preamble.

Criminal Procedure Code, (1898). s 154.

Electromagnetic Merriamwebster (2011). < https://www.merriam-webster.com/dictionary/electromagnetic> last accessed 10 October 2021

Police Order, (2002). Art-6.

NAB Ordinance, (1999). s 6.

Prevention of Electronic Crime Ordinance, (2007). Preamble

Prevention of Electronic Crime Act ,2(016). s 2b.

Prevention of Electronic Crime Ordinance, (2007). s 30.

Police and criminal evidence Act, (1984). Preamble, s 19.

Rowlingson, R. (2010). Forensic Readiness ADFS conference on digital forensic, *security and law*, 2(3)

NJI special report, electronic crime scene investigation, a guide for 1st responder (2nd edn) <www.ojp.usdoj.gov/nij>

The investigation for fair trial Act, (2013), Preamble.

The Constitution of Islamic Republic of Pakistan, (1973). Preamble.

The investigation for Fair Trial Rules, (2013). r 3 to 5.