

# Legal Procedure of International Computer Forensics Authorities

---

*Article by: Adil Waseem*

Computers have dramatically changed the means of communications and there has arisen new situation where traditional standards of gauging reliance of evidence have been defect owing to emergence of computer crimes. These crimes are related with electronic credit Cards and ATM fraud, misuse of Trade marks, e-copyright infringement, cyber hacking, etc. and these offences are committed by means of computer related tools and equipments which are extremely difficult for administrators of justice to comprehend the nature of offend and collaborating evidences presented for prosecution of these offences. In these complicated situated the assistance of computer forensics authorities are sought for arriving at correct opinion about digital evidence.

These impartial computer forensics authorities have been the part and parcel of legal system developed countries that provide all litigation function at request of courts and their services can obtain for getting computer evidences. The procedures of these authorities are regulated by special enactments according to the nature of offence committed. There are given statutory powers to identify, collect, produce, certificate and present written electronic reports in civil and criminal trial for administration of justice. These computer forensics authorities perform their legal duties regarding digital discovery of the e-documents.

When we look into the legal history of these computer forensics authorities, these were used in the course of prosecution for over twenty-five years in United State and in last decade, the numbers of computer forensics authorities were given license to establish their impartial set up for certify all documents produced in digital form developed with advanced with electronic communication to the investigating agencies and to court of law. The functions of computer forensics were given statutory powers for purpose of getting forensic view about the e-data or electronic evidence.

The Computer Forensics authorities' employs various procedures and tools for purpose of verification of documents, tracing the nature of offence from identification, collection and verification of electronic documents. After adoption of the complicated procedure they present legal version of these electronic documents in paper based form for admission before court of law. These functions are not limited to local disk data but even the remote server data is verified for purpose of gauging the veracity of these documents. The authentications of e-records from local hard drive to remote server are done in numbers of computer operating systems.

These procedures are adopted by the computer forensic authorities governed by prevailing law of state regulating the internal structure of these authorities. The identification is first step towards the electronic discovery and its likely sources of relevant information comparing it with original electronic documents. The identification of computer documents and its comparison with original record through critical step to ensure that data is not overlooked and each aspect of date is properly maintained and there is no tampering of database while its production before court of law for just adjudication of matter meeting the legal standard provided by the legal system. The views about the electronic document are requested of disk or remote documents and to inventory of the data and to look for hidden sources of deletion or tampering of e-records. In many cases, they present written e-discovery reports of cyber space and electronic communications and its links with database where it has been hosted or linked.

The Collection of electronic documents is only the first step for proper identification of website link with database. Once it is identified, then they precede steps towards that they have to follow and gather the relevant information for authentication of the electronic evidence as to judge the reliance of these evidences. They collect relevant information for coming to right conclusion regarding the authenticity of e-documents. They adopt numbers of modern devices to avoid the tampering of records and to maintain defensible protected documents. The critical procedural phases judge the reliance of the electronic evidence and its presentation and admission before the concern courts. The Computer forensics authorities employ internationally recommended devices for written protocols and internal procedures to ensure that stands scrutiny in all court jurisdictions where these are presented for purpose of admission of these e-documents. There are many hidden sources of electronic evidence that can not be retrieved without seeking the assistance of the authorities of foreign jurisdiction and in number of criminal cases, the coordination are done through international protocols and agencies. Once information the regarding the evidence existed out of state jurisdiction is gathered, document must have to follow the same procedure of as mentioned above.

In number of international license of computer forensics authorities, they are often license holder numbers of jurisdictions for collection and acquisition of true electronic records. The questions out of state jurisdiction does not arise in case international reputed computer forensics authorities. Rather it is foreign jurisdiction or not, important information is not retrieved without tested forensic procedures and documentations. The computer forensics authorities helps courts to avoid any unnecessary and uncertified production of documents, while ensuring that potentially relevant documents are presented, including encrypted, compressed, and password-protected files, are presented before court properly in accordance with the law of respective State for prosecution of the offenders.

Another procedure is used that of filtering of electronic database collected in electronic discovery while undergoing search of the electronic evidences. The computer forensics authorities employ the variety of methods, tools and

appropriate search technique to Windows and other operating system for increasing reliability of electronic documents for just adjudication of matter. The electronic forensics authorities are given numbers of statutory powers in the matter connect with assessing the reliance of the electronic and figuring out the hidden sources of evidence connected dispute in question and offenders involved in commission of these electronic crimes.

The admission of electronic documents before the court of law is primary function of these forensics authorities. The computer forensics authorities produce legal documents of certified documents to court of law and they also collaborate with investigating agencies in reaching right conclusion about act or omission on part of electronic offenders. They are granted certification power by statute or they are working independent autonomous bodies being famous for their impartial reports, they are often asked by court to give opinion about the electronic documents having agreed by parties to suit. They produce copies of the data selected for review and offer recommendations and certification regarding the nature of electronic database to be viewed as evidence meeting all standards of its admission.

The computer Forensics authorities perform numbers of other functions, one of these are offering detailed written certified reports and analyses to courts to just adjudication of matter and for fair prosecution of electronic crimes offenders. As being declared as expert's reports, they assist judges with the interpretation electronic evidence being presented in court proceedings and the testimony of other electronic discovery experts. The court often needs the opinion of these experts regarding the building of the electronic evidence and reliance. For getting appropriate and meeting the reliance standard, although careful attention to detail in the early stages of electronic discovery builds solid expert testimony.

The real aim of computer forensics to assist the court in reaching just conclusion regarding production of data as evidence but in Pakistan we have not yet legislated on role of computer forensics as expert role for identification, production and its admission before the court of law. Currently no Computer Forensics Authorities are running their business in Pakistan, reason may be, and no efforts are made to provide legal framework for establishment of certification authorities or to discuss the economic measures for their promotion. Here need to encourage the computer forensics authorities in Pakistan for getting accurate information for digital evidence. Their services can be obtained by contractual basis, or they can be incorporated in legal system as confirming them special substantive and procedural powers. The specific amendments should be made to incorporate computer forensics authorities into substantive, evidence and procedural laws to make the courts technically and legally able to deliver best judgment on issues affecting the electronic records. The writer is an advocate of High Court and practicing immigration and corporate laws in Pakistan since September 2001. Author can be contacted by Adil Law Company (Advocates and Immigration lawyers) Office No.3 2nd Flr Hafeez Chambers 85 The Mall Rd Lahore Pakistan Telephone: +9242-6306195 +9242- 6360108 Fax: + 9242 6360108 Cell: +92300 4254910 E-mail: adil.waseem@lawyer.com