Digital Forensics

Paving the way to preserving evidences critical to decisions in cybercrime investigations

Edited by
MOHAN DAS VISWAM

The role of Digital Forensics and subject expert is very decisive in the investigation of crime and further securing producible evidences before the judiciary without affecting the originality of evidences.

SB SINGH
Dy. Director General
sbsingh@nic.in

Dr. SURINDER KUMAR
Sr. Technical Director
suri@nic.in

DEEPAK GOEL
Sr. Technical Director
dpk_goel@nic.in

NK PRASAD
Technical Director
nk.prasad@nic.in

We live in an era of digital revolution in which Information Technology touches day-to-day activities mankind delve in. The socio- economic fabric has been immensely benefitted by the IT intervention, and the judiciary is no exception to this. The penetration of IT in the legal ecosystem has created an intense impact and has turned to be vital in various facets of the criminal justice system such as enquiry, investigation and prosecution. As per the legislation, these are laid down in the Information Technology Act 2000.

What is Digital Evidence?

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. The digital evidence or electronic evidence as such can be found in any electronic device such as computer hard drive, a mobile phone, a CD, a Personal Digital Assistant (PDA), as an electronic record.

IT Act 2000 on Digital Evidence

Electronic record is defined under section 2(1)(t) of Information Technology Act 2000 as data, record or data generated, image, or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. An amendment to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in the electronic world.

Before accepting digital evidence in judiciary, it is vital that the determination of its relevance, veracity and authenticity be ascertained and the fact whether it is hearsay or a copy chosen to the original be established.

Digital evidence is not only limited to computers but may also extend to other digital devices such as telecommunication or electronic multimedia devices, e-mails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, contents of computer memory, computer backups, computer printouts, Global Positioning System (GPS) tracks, logs from a hotel's electronic door locks and digital video or audio files.

Role of Digital Forensics

With rapid increase in IT implementations, cybercrime has also spread its wings in diversified fields and related areas as today, physical locations and distances are immaterial in cyberspace. Cybercrimes like hacking, cyber terrorism, cyber stalking, spamming, cyber pornography, phishing, spoofing, worm attacks, code theft, credit card frauds etc., are the nuisances with which human beings are living with.

A digital forensic expert is the key to any cybercrime investigation because cybercrimes may not be proved without them and criminals may get scot free. Thus, the prime role of a digital forensic expert is to acquire, analyse and report the digital evidence, which may help in proving the crime.

These tasks are conducted with the help of various forensics toolkits such as write blockers, forensic media card reader, forensic duplicators, lab forensic imaging/ cloning for data acquisition and software with high-end forensic workstations. Among the forensic software, EnCase, UFED etc., are widely used. CDAC has developed various forensic software tools touching digital forensics aspects. However, the usage of these tools depends on their features, ease of use and the exact requirement in a specific case.

Digital Evidence Life Cycle

As the electronic records can be easily manipulated, steps must be performed in a systematic and timely manner, safeguarding the integrity of the evidence by maintaining the "chain of custody". The admissibility of digital evidences in judiciary is very much dependent on the authenticity of evidences.

In order to ensure that a digital evidence is collected, preserved, examined or presented in a manner safeguarding its accuracy and reliability, law enforcement and forensic organisations must establish and maintain an effective quality system and documentation of each process related to the evidence. The effective quality system can be obtained through documented Standard Operating Procedures (SOPs) for quality-control guidelines that must be supported by proper case recording and use of broadly accepted procedures, equipment and materials.

The chain of custody of digital evidence is a crucial aspect during digital investigating process. It is initiated with acquisition of the evidence collection that should have an appropriate legal sanctity. The process of acquiring digital evidence begins under the well-laid-out legal procedure. This process differs from country to country, in relation to who first comes into contact with digital evidence. In some countries, there are specialised units (first response task forces) that are trained on how to handle such types of evidence, while in some countries such jobs are undertaken by law enforcement personnel (specialised police officers) with the help of digital forensic experts.

The initial phase in the life cycle of digital evidence is Identification and Collection, as the files that may have evidence are already created and present in the computer systems. In this phase, digital forensic investigators have to explore the enormous amount of material to find valuable evidence related to the spurious activity. This phase is very complex and time-consuming and there are more chances that chain of custody of that particular evidence is violated.

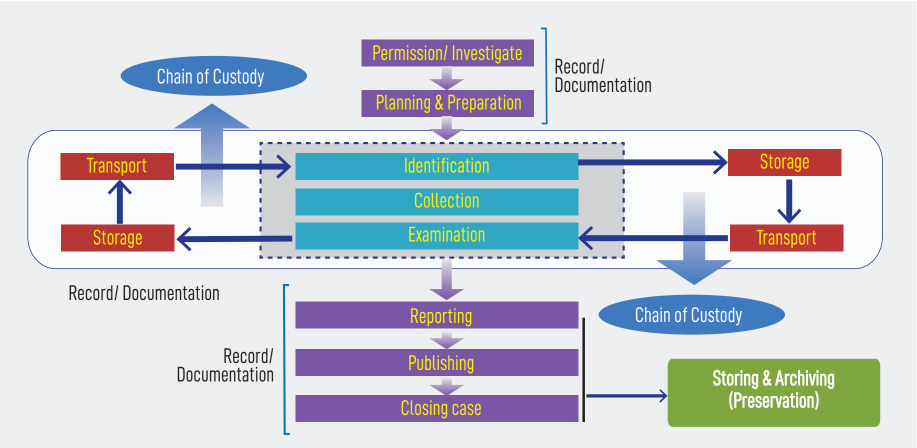
Next stage of the life cycle is Examination wherein the contact with digital evidence can happen by the forensic investigators and an expert witness. Examination phase implies the identification of potential digital evidence and separation of other large amount of digital files.

Next phase in the lifecycle is Reporting/ Publishing. In this phase, digital evidence is presented by the defence/ prosecution side, and contact with digital evidence can take place by the forensic investigators, an expert witness, defence and prosecution. The result of forensic investigations is presented to the court. At the end, digital evidence needs to be stored and archived (i.e., preserved) for almost a perpetual time or till the case is out of its life cycle.

The storage and movement of digital evidence has to be on a secure network and servers with access to the authorised personnel only, so as to maintain its authenticity and sanctity.

Preservation of Digital Evidence

The preservation or storage of digital evidence is an important aspect when deciding its admissibility in a trial in process, or in any future processes of case life cycle. The issues with the digital evidence, when extracted from the storage and played/ displayed as an exhibit in the court, which may be in a large number to handle, may range from the availability of the hardware, system software, application software to the non-operation of the digital evidence. In future, the availability of three infrastructure requirements (hardware, system software, application software of the same make and configurations) is a big challenge. In reference to software purposes, the solution lies in the building of software reference library, which can store all kinds of system software, application software etc. These packages may include multiple versions of various operating systems, database management systems, utilities, graphics images, component libraries etc. This library enables easy access to a collection of software packages required by forensic experts and can serve as a help for the purpose of producing evidence in the court.



Chain of Custody and Life Cycle of Digital Evidence

Tools and Technologies

A digital forensic expert must be equipped with requisite forensic toolkits such as write blocker, forensic media card reader, forensic duplicators and forensic imaging/ cloning software to acquire electronic evidences in order to maintain chain of custody. The digital forensic expert or litigants collecting the electronic record have to use appropriate data extraction tools and data compression or replication tools under defined protocols and generate the HASH value of the removable device and the electronic record. Other than the hardware implements, specialised software tools can also be used by experts as they not only help maintain the chain of custody, but also help the examiner sifting through the digital mesh created in a device.

Summary

Digital evidence, generated in any electronic media, can be of high importance in any criminal investigation, owing to a cybercrime as well as for the purpose of maintenance, debugging, data recovery from the computer systems in any organisation. Further, the setting up of infrastructure and processes involved such as reception, examination and reporting can strengthen the security of the IT infrastructure of an organisation. ■

For further information, please contact:

SHYAM BIHARI SINGH
Deputy Director General
Digital Archiving & Management Group
NIC, A-Block, CGO Complex, Lodhi Road
New Delhi - 110003

Email: sbsingh@nic.in
Phone: 011-24360788