Volume 9, April 2020 ISSN 2581-5504

"Digital Evidence and Cyber Forensic Procedure and its Role in Criminal Justice System"

***Hemangini Shekhawat**
Manipal University, Jaipur

****Deeksha Sabharwal**
Manipal University, Jaipur

DIGITAL EVIDENCE MEANING

Digital Evidence or computerized evidence is a kind of corroboratory/substantiating type of data restored or transferred in a conformational manner that a party to case may use at court. [1]The scope of computerized evidence has increased in part few years as Court of Judicature has allowed electronic mail, digital images stored, bank transactions, log history, text communication history contents or particulars of Computer/ Laptop/ Macbook memory/ printouts/ backups.[2]The data isn't allowed to be procured in a right way until and unless the gadget has been taken under control. For eg digital evidences are basically concealed up like fingerprints/DNA and can also be modified, reshaped and are also clock sensitive.

Before taking of evidence inn, court will decide the significance and pertinence of evidence and based on materiality will only allow the evidence later. Statistics is stored on computers, laptops, macbooks, smart android mobiles, Iphones that have storage capacity. [3]It also comprises of hard storages like Hard Drives, CD,DVD, Pen Drive, Floppy Disk including routers, drivers and iclouds. Type of information includes text messages and media. Statistics acquired from computerized devices can give crore amount of information.

Statistics can be acquired and used for intelligence purposes or to be served as a piece of evidence in Court of Law. Gadget generated content can be admissible in court if proven that security and privacy procedure were present to avert changes/ modification in data.[4]When content is both produced by a device or a user, its solidness has to be established in order to be relied upon.

HISTORY OF DIGITAL FORENSICS

Important milestones from history of digital forensics are [5]

- Harrs Gross(1847-1915) invented use of scientific experimentation to lead criminal investigations.

[1] https://en.wikipedia.org/wiki/Digital_evidence
[2] www.forensicsciencesimplified.org/digital
[3] https://www.definitions.net/definition/digital+evidence
[4] https://www.unodc.org/e4j/en/cybercrime/module-4/Key-issues/digitalevidence.html
[5] https://www.guru99.com/digital-forensics.html

Volume 9, April 2020 ISSN 2581-5504

- Federal Bureau of Investigation (FBI) layouts research labs to provide forensic assistance to field agents and other law authorities across United States Of America.
- In 1978, the foremost computerized crime was acknowledged under Florida Computer Crime Act.
- Sir Francis Galton (1882-1911) directed first recorded analytical study of finger prints.
- In 1992, Computer Forensics was used in scholastic arts/writing.
- In 1995 International Organisation on Computer Evidence (IOCE) was founded.
- In 2000 initial FBI Regional Computer Forensic Lab was inaugrated.
- In 2000, "Best Practices for Computer Forensics" was published as a text book by scientific working group on Digital Evidence.
- In 2010,(SWGDE) issues in regards to Digital Investigation were recognized by Simson Garfinkel.

SOURCES OF DIGITAL EVIDENCE

Sources and traces of Digital Evidence are as follows[6],

- Floppy Disk,
- Hard Drives,
- Answering Machines,
- Telephone messages storage,
- Electronic Diary,
- CD,
- DVD,
- Flash Drives,
- Pen Drives,
- Phones,
- Ipads,
- Ipods,
- Macbooks,
- Fax Machine,
- Scanners,
- Printers,
- Whatscan for Whatsapp,
- GPS High Frequency Direction Finder.

[6] https://www.slideshare.net/raghurx/digital-evidence-by-raghu-khimani

Volume 9, April 2020 ISSN 2581-5504

Latest digital evidences are as of following kind,

- USB Cookies,
- USB Cork,
- USB Teddy Bear,
- USB Gun,
- USB Pen,
- USB Watch,
- USB Debit Card/Credit Card,
- USB Burger,
- USB Food Dishes,
- USB Transports,

TYPES OF DIGITAL EVIDENCE

1. Volatile Digital Evidence

Volatile Non Persistent Digital Evidence are only present when PC is plugged to power. Includes internal storage memory and RAM which is alive only in computers system memory. Its required to be preserved otherwise. Statistics reserved in memory will be drifted if loses power. To prevent losing Volatile evidence the device must be continually charged. A mobile/PC must be plugged into power unless a forensic expert comes to the recue of its memory. [7]To regulate what evidence to collect first, an order of Volatility must be sketched up first,

a) Registers and cache,
b) Routing tables,
c) Arp cache,
d) Process table,
e) Kernel Statistics and modules,
f) Main Memory
g) Temporary file systems,
h) Secondary file systems,
i) Router Configuration,
j) Network Topology.

[7] Flylib.com/books/en

Volume 9, April 2020 ISSN 2581-5504

2. Non Volatile Evidence
   Evidence is available even if PC ain't plugged to power. [8]Includes external storage like tape, floppy disk, hard drives, CD, DVD. Irrespective of non persistence data is still reserved in memory. Storage is basically done in semi conductors memory chips which stockpile data in floating gate memory cells comprising of floating gate MOSFETS including flash memory storage.

PURPOSE OF DIGITAL EVIDENCE

The rapid mushrooming and the impact of information technology on humankind as a whole conjoined with the expertise skill to stockpile and amass details and particulars in digital form having all demanding alterations in domestic laws (Indian Laws) to subsume the provision on the acknowledgement of digital evidence.[9] The Information Technology Act,2000 and its rewriting of laws is based on United Nations Commission on International Trade Law (UNCITRAL) model law on electronic commerce. The Information Technology Act,2000 was rewritten to permit the preparedness of digital evidence. In computerized world the legislative substructure is provided by the amendment in Indian Evidence Act, 1872, Indian Penal Code, 1860 and the Bankers Book Evidence Act, 1891. Digital Evidence is any corroboratory confirmative data stored restored pr transferred in digital form that a party to a litigation may try at. Before accepting digital evidence its crucial that court may test it and determine its relevance, accuracy and truthfulness along with also to establish if the fact is hearsay or a copy of original. Digital Evidence is data/ statistics of substantiating value that is restored or transferred in binary form. Restriction isn't only on the evidence found in computers but also include evidence on telecommunication or automation or electronic and other mixed media devices. Email, digital photos, ATM Transactions, Log Files saved from accounting program computer backups, computer printouts, contents of computer memory , GPS tracks, logs from hotels electronic doors, Digital Video/Audio files are all sources of E-Evidence. Digital Evidence tends to be more capacious, more strenuous to demolish, easily altered, easily copied, probably more expressive and more readily available.

DIGITAL EVIDENCE AND ETHICAL ISSUES

Digital Evidence is Any information which is derived from a device (Mobile, Computer, laptop, Hard Disk) and can be used as a proof for legal proceedings. However, it needs to adhere to certain rules. Evidence is something which can be used to prove a fact in the court of law. Digital

[8] https://en.m.wikipedia.org
[9] https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali

Volume 9, April 2020 ISSN 2581-5504

Evidence as the name suggest is in electronic form which is originated for electronic sources, namely: Mobile, Smart watch, Laptop. I Pad, Desktop, Hard Disk, etc.

- **Legal Authority-** It becomes very necessary that the forensics examiner must have the authority to identify, analyze, collect and preserve the data/ information in digital format.
- **Fragility-** If the evidence is not collected, preserved or protected properly by the forensics examiner, it may lose its value as data can be altered or tampered easily depending on its source.
- **Admissible-** Evidence is of any use/ value if it is valid and admissible to the court/ judge or jury. If the data is preserved and is in good condition, but is of no relevance to the case, would not be admissible as no decision can be made on the basis of that. Admissibility of any digital evidence can be judged by its
  - Authenticity
  - Reliability
- **Validity-** Validity/ accuracy/ correctness of data or evidence or information can be determined by the tools and processes which are used in the forensics examination.
- **Credibility-** Controlling standards, guidelines and tools used for collecting the data are means to demonstrate its credibility.

ADMISSIBILITY

The continuous development of technology is achieving milestones with new and improved devices like, Mobiles, laptops, etc. and have become a major part of society which has led to the creation of physical data.

With rapidly changing technological environment the role of digital forensics experts is also playing a crucial part as the information derived from digital devices can be used as a concrete evidences in cases such as terrorism, cybercrime, hacking, robbery. This data can be recovered or accessed from various digital repositories such as cloud network, USB drives, telecom networks, emails, internet history, etc.

The collection process for evidence is:

1. Collecting the data/ devices as per mentioned guidelines.
2. Analyzing the data with the help of the best and verified equipment, and
3. Reporting the data in a way that is admissible of court of law.

Negligence to any of the mentioned steps or their related guidelines or process could lead to loss of authenticity of data/information which might not be admissible of court.

Volume 9, April 2020 ISSN 2581-5504

PRINCIPLES OF DIGITAL EVIDENCE

There are several guidelines and practices which are developed by Scientific Working Group on Digital Forensics, UK Association of Chief Police Officers and US National Institute of Justice. There guidelines, having been developed in order to help and guide the digital forensics experts, says:

1. No evidence or data or information should be tampered or altered as the court may rely on it's for the proceedings and judgement.
2. If under any circumstance the device containing the data need to be accessed, then the respective digital forensic expert should be capable enough to ensure that the data does not loses its authenticity and should also be able to explain the same to the court.
3. Also, all the processes applied on the device containing the data should be recorded in step by step and preserved. Same would be used to a third party to Audit the evidence by performing the same step by step process in order to achieve the same result.
4. It would be responsibility of Investigation officer to ensure that all the guidelines are being followed and in case of any deviation he would be held responsible.

KEY POINTS FOR HANDLING EVIDENCE

1. Auditability- As mentioned earlier, all processes applied on the evidence should be recorded step by step in order to ensure that the same results are derived when those steps are followed by a third party.
2. Justify- All methods used to handle the evidence should be justifiable by the investigator and he should be able to demonstrate that the method chosen is providing the best results.
3. Repeatability- The authorized person should also be able to perform the tasks.
4. Reproduce- Under different environments the result of the test should not change.

   Any evidence is admissible when it is able to prove the fact of the case; and, does not violate any legal statutes. Any evidence which is relevant is admissible and any evidence which is irrelevant is in admissible in court. However, the judge can carry out the legal tests to identify the admissibility.

1. Evidence Obtained illegally- Evidences which are related to the privacy of a person might not be admissible in the court unless it is an important evidence and has been obtained as per protocols.
2. Authenticity- if any evidence is altered it would lose its authenticity. Authenticity can be maintained by avoiding un necessary access to device containing evidence. Also authenticity can be validated by hashing the code of the evidence.

Volume 9, April 2020 ISSN 2581-5504

3. Reliability and relevance- Court can ask an IT Expert or a third party representative to follow the steps used by the forensics to derive the same result as that of the evidence to ensure that there is no deletion or alteration of evidence.
4. Search warrants- investigating teams need to have proper authorization for collecting the evidence. If it is collected without any authorization, it may result as in admissible in court.
5. Scientific Process used on evidence- It is very likely possible that the methods and techniques can be challenged in the court.
6. Tangible evidence- to support the digital evidence some tangible supporting evidence can be used such as report on the series of actions taken. Finger print reports, etc.

Digital forensics is playing a very important role in the judicial system by:

- Reducing the time taken to analyze and process the evidence,
- Cyber Security
- Protection of intellectual property rights and financial information.

However, it is also offending the Privacy of individual.

There has been a decent development in considering the digital evidence as admissible in court. In 2003, in a landmark case of Twentieth Centrury Fox Film[10] several safe guards were laid down by Karnataka High Court:

1. A witness should file an undertaking in order to confirm that he is the same person on the screen. This undertaking is to be filed in the presence of a Notary or Judge.
2. The person who would be examining the witness on the screen also needs to file an undertaking in order to confirm his identity.
3. No Examinations is to take place beyond the working hours of court.
4. Witness has no rights to plead any inconvenience basis the different time zones followed.
5. The remarks must be recorded by a Judge along with the objections raised by the witness. Same would be used in court during arguments.
6. Once the recording is complete, a copy of it is to be given to the witness and his signatures is to be done in the presence of Notary post which it would be used in Court.
7. Also the witness needs to alone at the time of recording and same is to be certified by Judge.
8. The Jude can also apply certain other rules and conditions, if required.

[10] Twentieth Century Fox Film v NRI Film Production Associates

Volume 9, April 2020 ISSN 2581-5504

9. All expenses are to be paid by the applicant.

In 2005, Bagchi case[11], Calcutta High Court held that, "it is to be remembered that by virtue of an amendment and insertion of Sections 65A and 65B of the Evidence Act a special provision as to evidence relating to electronic record and admissibility of electronic records has been introduced with effect from 17th October, 2000. Consequential amendments are also made therein. Therefore, there is no bar of examination of witness by way of Video Conferencing being essential part of electronic method"

In 2007, case of Bodala Murali Krishna[12],the Andhra Pradesh High Court has allowed the use of Video Evidence stating that Video evidence can be used in Civil Case provided they meet and follow the same standards as that of the Criminal case.

COMPUTER FORENSIC DEFINITION

It is a limb of forensic science relating to legal evidences found in computers, mobiles, laptops, tablets. Computer Forensic is also termed as Digital Forensics. The aim of Computer Forensics is to detail the current state of a digital artefact. Digital Artefacts involves firstly computer system storage medium (hard disk, CD Roms) and secondly is Electronic document (Email, Whatsapp) and lastly is Trail of Packets moving over computer. Definition of evidence has been altered to also comprise electronic data. The documentary evidence has been now changed to include all documents, including electronic records produced for inspection.

CYBER FORENSIC PROCEDURE IN CRIMINAL JUSTICE

At the opening level, the claimant reaches cyber crime police station or to a police station if cyber crime police station doesn't exist. If the offence stands to be a cognizable offence, the essence and the modus operandi of crime regarding particulars shall be recorded up in complaint. For eg, Copy of defaced web (Soft Cover+ Hard Cover).

After what follows is preparatory analysis and evaluation of the entire scene in order to expose potential evidence. After that a conservation notice is sent to all parties thereafter to protect the evidence (only connected parties). To ensure uprightness of the evidence and to prevent tampering of same, confinement steps are taken up. For eg. Quick freezing the bank account of accused to avoid further money frauds.When the collection of evidence starts the procedure has to be followed with live on systems and live off systems to be complied with hunt and annexation under Sec 165 of Criminal Procedural Code and Sec 80 of Information Technology Act along with mirrored in Panchnama. To guarantee the probity of digital evidence Hashing is a

[11] Amitabh Bagchi v Ena Bagchi
[12] Bodala Murali Krishna v Bodala Prathima

Volume 9, April 2020 ISSN 2581-5504

commonly used technique. It encloses "Crypotographic hash role Break through" and is a sort of mathematical way which is "based on an innovation which makes a digital portrayl often referred to as cryptographic message digest which is compact but nonetheless distinctive in its own nature". Digital evidence collection form is used to store the documentation of evidence comprising of procedure, instruments used, values obtained from forensic images of evidences.[13] Aside from being important measures in impacting evidential value of algorithmic evidence, existing the chain of custody and a confirmation data of the same is in essence of a mandate on Investigating Officer, reason being Investigating Officer will be liable for legal actions against criminal liability under Sec 72 of Information Technology Act 2000 for its infringement.

After gathering and documenting the evidence in following ways either by forensic imaging or been restored in USB, Hard Drive, Floppy Disk, TV, the proofs are sealed and reequipped in evidence data base. Court orders are awaited thereafter to send the evidential proofs for forensic examination. In case, where holders of property approaches court for liberating the evidence, the Investigating Officer rather then providing original authentic copy of grabbed evidence, should provide copies of forensic imaged. Apart from these conductal obligations, inspecting other external information effecting same. For eg, When systems are attacked beyond the regional time zone, time zones transmutations are relied upon then for reassembling case in total, other external data from web and e devices are also to be relied upon in total.

CYBER CRIME INVESTIGATION BY CENTRAL BUREAU OF INVESTIGATION

Central Bureau of Investigation can be approached at all times for all sorts of crime whether serious or not in nature for finance related crime, it has economic offence cell to investigate the same for the function of combating crimes. CBI has expertise structures for same.

1. Cyber Crime Research and Development Unit, (CCRDU)
2. Cyber Crime Investigation Cell, (CCIC)
3. Cyber Forensics Lab, (CFL)
4. Network Monitoring Centre.

1. Cyber Crime Research and Development Unit (CCRDU)
   CCRDU is mainly encumbered with a work of gathering details and particulars on computerized cases announced for further look up in collaboration with state law enforcement officers. On a bigger jargon, it plays crucially centred role in gathering and communication of all particulars on cyber crime in pally with Ministry of Electronics and Information Technology, Government of India and other agencies and Interpol Cyber Bases. Police and people are continually subservient on delegated IT agency which are headed by practiced and experienced cyber security specialists who discover proper inspecting

[13] www.online.norwich.edu

Volume 9, April 2020 ISSN 2581-5504

protocols and make device meticulous training plan of actions to assure finest plans of action are followed in superintend way. In plus to finding severe course of action to be taken for forensic procedure, Internet security divisions must also frame away regulations for administering all e-activities within an organization.

2. Cyber Crime Investigation Cell (CCIC)
   CCIC has capacity to investigate the delinquent acts of crime under Information Technology Act, 2000 and is also prong of proximity for Interpol to delineate the cyber crimes in India. A cue component of the Investigative procedure involves the evaluation of prospective proofs in cyber crime. Efficacious organizing of evidence is a clear mastery of particulars of case at point and also categorization of computerized crime in question. For eg. If a department has to seek to prove to prove that a person has perpetrated to commit crime in relation to identify theft, then computer forensic examiners desire suave and polished ways to sleeve through social networking sites such as facebook, whatsapp, email, hangouts, storage devices as CD, floppy disk, DVD, flash drives to repossess and regain any sort as evidence which can aid as achievable and accomplishable evidence of crime. This is obviously alike like other crimes where criminal shares fake products on fake shopping websites to procure credit card and other financial details. Preliminary of conducting an investigation, the investigation must describe the kind of evidential proofs sought and of how to conserve the same. The investigation should also study the source and authenticity of such data.

3. Cyber Forensics Lab
   CFL being third organ provides deliberation and does criminal investigation for various law implementation agencies. It not only furnishes onsite backing ups for computer hunt and invasion but also yields specialised testamentary verification in court of law. Its relevant to see that CFL must also be abiding by all legal obligations during subjugation of media for making the same in court of law. Chain of custody should be implemented & maintained and the probe should be related on depiction of media. Perchance the most censorious facet of successful analogue. Forensic investigation is a meticulous and elaborative process to procure evidence. Substantial substantiation is required before to, during, and after the procuring process, full particulars must be preserved and presented including all equipment and operating system, any apparatus used in investigation procedure and the apparatus being investigated. Procuring evidence must be skilled in a manner both purposive and legitimate. Being capable to certify and validate the chain of evidence is very important while pursuing a court case and this is very true for forensics. Keeping the probability of distant ingress from an isolated location across the universe into contemplation, the statics storage is another dominion cannot be regulated out all together. In circumstances involving the data

Volume 9, April 2020 ISSN 2581-5504

location in another nation, the Interpol has to inform as a pre requisite and also abiding Sec 166 of Criminal Procedural Code.

4. Network Monitoring
   To scan the internet usage by various tools network monitoring plays a great role. [14]It scans the usage and notifies the administrator. Network Tomography, is a crucial domain of network measurement observing the soundness and robustness of various links using end to end scrutiny sent by proxy factors located at vantage points in the internet network.

CONCLUSION

The question on the admissibility of the Digital Evidence/ Electronic Evidence, stands answered by the judgements of various High Courts and Apex Court over a period of time. Section 65 B also clarifies the conditions which needs to be fulfilled in order to make a digital evidence admissible in court. However, the question still arises if a digital evidence such as a video recording of the accused in the presence of Judge can be used against the accused as the sole evidence?

[14] www.en.wikipedia.org/wiki/Network_Monitoring