International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 20-01-2024, Accepted: 12-02-2024, Published: 06-03-2024
Volume 10, Issue 2, 2024, Page No. 18-22

Analysis on admissibility of digital evidence in present era in the context of Bangladesh

Roshna Zahan Badhon
Lecturer, Department of Law, Primeasia University, Bangladesh

Abstract
As the world has turned up into its new frontier of digitalization, laws are also be innovated according to the modern changes. Digital crime has been increased in recent time. To prove digital crime we need to place digital records as evidence in judicial body otherwise justice cannot be secured. In past it was very unfortunate that no country had any clear concept of considering digital records as evidence, even though there was no treaty or agreement regarding this concept. The Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensics called 'Best practices for Computer Forensics' in 2002. Moreover the ICC has developed digital evidence standards to meet up the needs. Many countries (i.e. India, Pakistan, UK, USA) have already introduced it in their judicial system based on some fruitful research. In Bangladesh the most leading case named Biswajit Murder Case is the case where digital evidence is admitted for the first time in the history of judicial system in Bangladesh when no other evidence was existed and from then we have found some more cases like this. Recently the Evidence Act, 1872 has been amended for the sake of giving admissibility of digital records in 2022. But the main challenge in this regard is to prove the authenticity of digital evidence. Moreover, it can be manipulated, erased and moved easily. Our courts should be reformed to consider digital records. Judges, experts should be trained properly, public awareness should be increased for using digital records as evidence.

Keywords: Digital crime, digital evidence, computer forensics, SWGDE, HM-DEAA, NIST, ICC

Introduction
Computers and other digital devices are used for committing crime, and, blessings to the blossoming science of digital evidence forensics, law enforcement now uses computers to fight with digital crime or cyber-crime in present era. Unfortunately the laws which we had did not recognize the admissibility of digital evidence previously. By the passes of time, methods of committing crimes are changing day by day. To overcome this situation we have now many laws where digital evidence is recognized as evidence in our court to meet up demands.

Concept of Evidence Law
The law of evidence is a vital element in legal proceeding for the judicial system of every country. It encircles the rules of legal principles that govern the proof and facts in a legal proceeding and plays a mandate role. According to Cambridge Dictionary evidence means and includes:- facts, information, documents, etc. that give reason to believe that something is true. Evidence helps to reach a fair & rational decision on certain point to ensure proper justice. The rule of evidence varies from case to case. The law of evidence has certain norms, standards, characters for each and every litigation in every country.

Meaning of Digital Evidence
The technological enlargement in the 21st century has refined the world. Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, among other devices. Digital evidence is commonly associated with electronic crime, or e-crime, such as child or adult pornography; credit card fraud etc. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects [1]. Digital evidence has probative value in a litigation.

Background of Digital Evidence
The birth of Digital Evidence has been a response to a demand for service from the law enforcement community. To meet the need the Federal Crime Laboratory directors in Washington DC formed a group known as Scientific Working Group Digital Evidence (SWGDE) in order to find latent Evidence on a Computer. The concept of digital evidence was proposed to federal laboratory directors on March 2, 1998. And for the first time in 2002, the Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensics called "Best practices for Computer Forensics [2]".

Objective of Digital Evidence
The primary goals of digital evidence are to assist in the recovery and preservation of computer and contemporary technology-related evidence to be used in court. In exceptional situation it can help to prove the fact in issue where there is no other way to prove the matter. One of the most paramount objects is to be able to recover the erased and removed files from digital media; extract them and validate long-lost items.

Types of Digital Evidence
To bring the guilty to justice, correcting, analyzing & presenting the right evidence is needed for every aspect to do justice. Before proceeding with the investigation we need to know where and how to look for certain digital evidence. For this purpose we need to know the varies types of digital evidence. Apparently we have found following 8 types of digital evidence in recent era [3]

- Logs

- Video Footage and Images
- Archives
- Active Data
- Metadata
- Residual Data
- Voltatile Data
- Replicant Data

According to my view as per above discussion we can figure it out through the following diagram

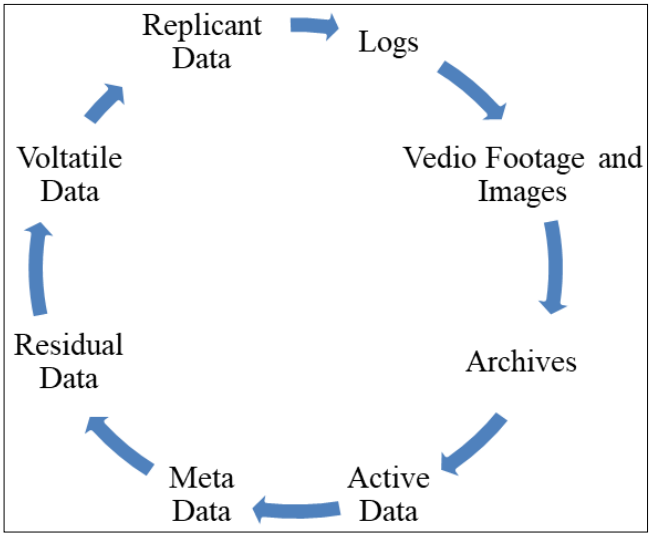

Diagram 1: Types of Digital Data

Significance of Digital Evidence

The development of science has made life a whole lot easier where information can be communicated, generated and stored electronically, and the development and progress of personal computers have also led to the development of crimes. An observation has been made in the Lorraine VS Markel case [4], where the Chief United States Magistrate Judge Grimm of the United States District Court of Maryland motioned that "because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try [5]." Hence, it can be presented in a way that without taking the aegis of electronic digital evidence, there cannot be a proper adjudication of most of the cases occurring in recent times. Despite being a parent statute, the Evidence Act 1872 does not accept digital documents as evidence. Because of this, the provisions' scope and applicability are limited and cannot be applied effectively to ensure justice and aggrieved cannot able to get proper remedy. As a result, Bangladesh now needs to officially incorporate digital evidence into its legal and judicial system. Bangladesh has seen the potentiality in cases like the ***Biswajit Murder case***, ***Rajon*** *Murder Case, Nusrat Murder, Abrar Murder case, and Rifat Murder Case [6]*.

Judicial Decision on the Admissibility of Digital Evidence in Bangladesh

Digital evidence is being used in every types of cases in our judicial system now a days. Although there is no specific and supporting law in Bangladesh governing the use of digital evidence, it has been observed in some of the most notable cases recognized by judicial body first. As previously stated the incorporation of digital evidence is required and can be achieved by amending and interpreting current legislation otherwise it is quite impossible to prove the guilty of an accused.

The definition of "any matter expressed or described upon any substance by means of letters, figures or marks" of Documentary Evidence is cited in section 3 of the Evidence Act 1872 [7], section 3(16) of The General Clauses Act,1897 [8] and section 29 of Penal Code, 1860 [9] can be interpreted to include digital evidence since the word "matter" is a term of the widest amplitude [10]. It further notions that Judicial interpretation articulates digital evidence as an amplification of matter expressed or described upon the digital substance by means of letters, figures, or marks and inclusive of material and secondary evidence and that it verbalizes the other forms of digitalization having a similar legal entity [11]. Now if the question arises of the authentication of digital evidence then there is the scope of expert opinion clearly mentioned in the Evidence Act,1872 section 45 where if needed the court can call for expert opinion. Furthermore, Section 165 and 161 of the Code of Criminal Procedure, 1898 also empowers the investigating officers to attach anything and examine and cross-examine the maker of the documentary evidence [12]. In one of the leading *Biswajit murder cases*, it was seen that the video footage of the incident was handed over to the investigating officer and its recording was also authenticated. So, it can be said that digital evidence is admissible in the context of Bangladesh and that there lies no bar to that [13]. In the Case of *Mrs. Khaleda Akhtar Vs. The State* [14] the prosecution wanted to introduce a video cassette as evidence in the petitioner's case. The trial judge granted the prosecution's request. Later, the aggrieved petitioner filed a criminal revision against the judgment alleging that the videocassette is not a document as stated in section 3 of The Evidence Act, 1872. Per Mr. Justice A.T.M. Afzal, the High Court Division provided a constructive analysis of the term 'matter' contained in Section 3 of the Evidence Act, 1872. He opined that the term "matter" occurring in the definition of section 3 is of the widest amplitude. He further added that if for the purpose of recording specific matter on magnetic tapes for the purpose of showing it on television by application of technology, a video cassette or tape is made, then we hardly see any reason why the same shouldn't come within the definition of document [15]. It was also pointed out in court that since sound recorded on a cassette may be used in court; there is little reason why a recording of sound and visuals can't be used in court as well. Thus, the court found no ground to not to hold video cassettes within the definition and meaning of the document of the Evidence Act, 1872 [16] In the case of *The State Vs. Qamrul Islam & Others* [17] reported in, Mr. Justice Md. Jahangir Hossain held that they also find it inclined to hold a video record footage within the meaning of document under the Evidence Act and is accordingly admissible in the court if otherwise relevant in course of a trial of the proceeding [18]. Moreover, by the virtue of current situation in Bangladesh Evidence Act, 1872 has been amended and new provision regarding digital record has introduced there [19].

Evidence Law on the Admissibility of Digital Evidence in Bangladesh

Evidence Act, 1872 had no provisions regarding the admissibility of digital evidence. Moreover, it did not

enlighten the importance of accepting the importance of digital records. Digital records were not recognized there [20].

According to Evidence(Amendment) Act, 2022- When the Court has to form an opinion upon a point of foreign law, or of science, physical or forensic evidence or digital record, or art, or art, or as to identify of hand writing or finger impression or footprint or palm impression or iris impression or type writing or usages of trade or technical terms or identity of person or animal, the opinion upon that point of person specially skilled in such foreign law, science, physical or forensic evidence or digital record or art, or in questions as to identity of hand writing or finger impression, footprint, palm impression, type writing, usage of trade, technical term or identity of person or animal, as the case may be, are relevant facts. Such persons are called experts [21]. It means our Bangladeshi law now has given intensive care in admissibility of digital records based on expert's opinion.

Effects of Considering Digital Evidence

The dimension of the prosecution to submit electronic evidence as direct and primary evidence in court is bottom line in light of ongoing global chaos. More than traditional kinds of proof, electronic records prove the accused's guilt. The benefits of electronic evidence may be very challenging to embrace. The courts must judge and verify the credibility of such evidence. *Ajmal Kasab's attack* was planned in person or via software. The prosecution used internet transaction transcripts to prove the accused's guilt [22]. The Indian Evidence Act has effectively blurred the line between main and secondary forms of evidence by including all digital evidence. While the distinction should still apply to other documents, a computer exception has been made. This is necessary since digital evidence is not easily producible in tactile form. While it is feasible to produce a word document in court without the use of printouts or CDs, it is not only difficult but impossible [23]. Criminals may be able to easily manipulate court records using electronic evidence in digitalized era. But technology has answered. Now computer forensics can cross-check when and how an electronic record was updated. Computers are today's most popular devices. A computer processor controls other equipment. Sections 65A and 65B [24] cover a lot of ground. The law allows any device having a computer chip to be used as evidence.

International Standard of Digital Evidence

There is no international treaty where we find the admissibility of electronic evidence. However, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce gives legislative advice at the UN level for countries to build their national laws [25]. To establish the admissibility of digital evidence, Antwi-Boasiako and Venter (2017) created the Harmonized Model for Digital Evidence Admissibility Assessment (HM-DEAA). Digital evidence assessment, consideration, and determination are all proposed in the HM-DEAA. To ensure that digital evidence is admissible in national courts, this framework underlines the legal and technical prerequisites [26]. The International Criminal Court faces issues as digital evidence becomes more common. The ICC lists four categories of evidential concerns that are unique to digital evidence: (1) authenticity; (2) hearsay; (3) chain of custody, and (4) preservation of evidence. Rule 69(4) of the ICC Rules of Procedure and Evidence directs the judges to admit evidence taking into account the probative value it carries with it for a fair trial and evaluation. Moreover, under Rule 63(2) the judges after evaluating all of the evidence in a case decide the probative value and "proper weight" of admitted evidence [27]. International criminal courts mix elements of common law and civil law traditions. The ICC has developed digital evidence standards. Even before the Confirmation Hearing, digital evidence and material must follow an "e-Court Protocol". The requirements under this e-court protocol are ensuring authenticity, accuracy, secrecy, and preservation of the record of proceedings. The Protocol demands metadata such as the chain of custody in chronological order, the source's identity, and the original author and recipient's organizations [28]. The ICC does not require a judge to rule on the evidence's authenticity. If the parties agree that the evidence is authentic or prima facie reliable, the judge may accept it. It was further ruled in Prosecutor v. Jean-Pierre Bemba Gombo, "A recording that has not been authenticated in court can nevertheless be accepted, as the Chamber considers multiple factors when establishing an item's authenticity and probative value [29]." Ad hoc tribunals, on the other hand, support external verification of digital evidence.

Application of Digital Evidence in United Kingdom

The Civil Evidence Act 1968 and the Police and Criminal Evidence Act 1984 set out requirements for the admissibility of certain types of computer-produced evidence. As part of the conditions of admissibility these statutes lay down minimum authentication requirements. However, the Acts arguably only apply to evidence that would otherwise be excluded as hearsay and not to direct or real evidence; in such a case the law contains no clear statements as to how that evidence should be authenticated [30].

Application of Digital Evidence in USA

The Federal Rules of Evidence 702 require that scientific and expert testimony must be reliable both with respect to the principles and methods used by the expert and application of the principles and methods to the specific facts. The original test for admissibility of scientific evidence was the Frye test (Frye v United States, 1923). The Frye test allowed scientific evidence to be admitted if the science upon which it rested was generally accepted by the scientific community. More recently, the Frye test has been replaced in federal courts by the Daubert test (Daubert v Merrell Dow Pharmaceuticals, 1993). Daubert held that the courts have a gate keeping obligation to assess reliability of scientific evidence. The Supreme Court proposed five criteria to determine the admissibility of scientific evidence: whether the technique has been tested, whether it has undergone peer review, whether there is a known error rate, the existence and maintenance of standards controlling its operation, and (like Frye) whether the technique is generally accepted by the scientific community [31]. The work of National Institute of Standards of Technology (NIST) is, for this purpose, very important. The field of digital evidence—both the devices to be exploited and the tools to exploit them—change rapidly. NIST testing provides the basis for asserting that the data gathered and analyzed by new tools is

scientifically valid. New advances in computer forensics technology will continually raise reliability issues, particularly as new techniques are deployed in the field without extensive review and testing seen in non-technological scientific fields. For example, one federal district court has found that testimony about the "granulization" theory of historical cell site data was not reliable enough to pass Daubert (United States v Evans, 2012) [32]. The court believed that an FBI agent could give lay opinion testimony about the location of cell phone towers in a particular area and the specific towers that an individual defendant connected to, as well as expert testimony about how cell phone technology works.6 But the agent could not testify about his opinion about the actual location of the phone, since there was significant dispute about whether a cell phone typically connects to the closest cell phone tower. defense was not "made in a reasonably usable form" but instead was done in a way "that disguises what is available, and what the government knows it has in its arsenal of evidence that it intends to use at trial" (United States v Stirling, 2012) [33].

Application of Digital Evidence in India

The landmark judgment of renowned case *Arjun Panditrao Kotkar v. Kailash Kishanrao Kotkar* has ushered in a new era of clarity and understanding regarding the admissibility of electronic evidence in Indian courts. This judgment stands as a shining example of the judiciary's commitment to upholding the intent of the legislature and its role as a pillar of support for the legal system and society at large [34]. As the realm of technology continues to evolve, the Indian legal system must remain adaptive and responsive, incorporating electronic evidence while upholding principles of fairness and justice in its courtrooms. This judgment serves as a beacon for the future, setting a precedent that will continue to guide and shape the admissibility of electronic evidence in Indian courts for years to come [35].

Application of Digital Evidence in Pakistan

Digital/electronic evidence is now admissible evidence in rest of the world, the criteria mechanism may differ from state to state but the point of admissibility is very much clear. Unlike other states Pakistan also tried to make amendments in law of evidence as per the needs and demands of trends set by the modern world and enacted several laws in order to complement the laws with the trends set by I.T, main contributions includes, the amendment (addition of some Articles and addition of some provisions in the existing Articles) in Qanune-Shahadat Order, 1984, promulgation of Electronic Transaction Ordinance, 2002, The Prevention of Electronic Crimes Act, 2016, Investigation for Fair Trial Act and Rules, 2013, Federal Investigation Act, 1974, Anti-terrorism Act, 1997 etc [36].

Comparative Analysis of Bangladesh and Global Regulations of Electronic & Digital Records

Aspect	Bangladesh (e.g. Evidence Act, Digital Security Act etc)	Global (e.g. GDPR, ECPA, FRCP)
Legal Recognition	Recognizes electronic and digital records and digital signature	Varies by country generally recognized
Admissibility Standards	Specific provisions in the Evidence Act for digital records	Guidelines for managing & admitting electronic evidence
Digital Signature	Legal Validity similar to physical signature	Digital signatures widely accepted.

Diagram 2: Comparative Analysis of Bangladesh and Global Regulations of Electronic & Digital Records

Recommendations

Though we have recognized the admissibility of digital records as evidence worldwide, we have to reform the system of litigation so that digital evidence can be proved easily for ensuring justice. For this *firstly*, we need to make suitable our courts for introducing digital records as evidence. *Secondly*, our judges and court staffs should be trained up in this regard. *Thirdly*, awareness of people regarding the use of technologies should be increased. Many campaign can be arranged for making awareness to the people about the positive use digital devices. *Fourthly*, digital evidence can easily be erased, modified, altered. *Fifthly*, IT experts should be required to deal with modern technologies. *Lastly*, law enforcement agencies must have a complete digital management system to overcome the situation of diversity of digital devices, data and volume.

Conclusion

Science and technology as well as law are vibrant and changing with moving civilization and digitization. In both civil and criminal cases evidence plays a crucial role for ensuring justice in legal system. Nowadays maximums crimes are committed by using digital mediums. For the purpose of ensuring justice admissibility of digital records as evidence is one of the most burning issues in present era. It can be used in the investigation and prosecution of matters. If we cannot recognized digital records as evidence we cannot do justice. Accused can be easily get rid from his punishment by not giving considering digital records as evidence. Justice system can be questioned in this regard. To overcome with these massive circumstances many countries in the world has introduced or amended laws. Finally in recent days we have found some laws regarding this issue in Bangladesh but proper measures and requirements should be taken while taking digital records. The importance of digital evidence cannot be overstated. For this reason we have an international standard of accepting digital evidence. Every nation should follow that standard in civil, criminal and cybercrime cases.

References

1. Digital Evidence and Forensic <https://nij.ojp.gov/digital-evidence-and-forensics> [Accessed on 20.02.2024]
2. Carrie Morgan Whitcomb. 'An Historical Perspective of Digital Evidence: A Forensic Scientist's View' [Spring], International Journal of Digital Evidence,2002:1(1):4.
3. What are the 8 Types of Digital Evidence? < https://www.salvationdata.com/knowledge/8-types-of-digital-evidence/ > [Accessed on 20.02.2024]
4. 241 F.R.D. 534
5. 241 F.R.D. 534

6. Khandker Saadat Tanbir. Admissibility of Digital Evidence in Bangladesh, 30 October 2021, BdJLS <https://bdjls.org/admissibility-of-digital-evidence-in-bangladesh/> [Accessed on 20.02.2024]
7. The Evidence Act, 1872 (I of 1872)
8. General Clauses Act 1897 (X OF 1897)
9. The Penal Code, 1860 (XLV of 1860)
10. Rajib Kumar Deb. Admissibility of digital evidence, [27th August, 2019], The Daily Star <https://www.thedailystar.net/law-our-rights/news/admissibility-digital-evidence-1790917> [Accessed on 20.02.2024]
11. Ibid
12. Rajib Kumar Deb N-10
13. 70 DLR (HCD) (2018) 26
14. 37 DLR (HCD) (1985) 275
15. Mohammad Shahjahan. Admissibility of Digital Evidence: Bangladesh Perspective, (15 January, 2022), Lawyers Club Bangladesh < http://lawyersclubbangladesh.com/en/2022/01/15/admissibility-of-digitalevidence-bangladesh-perspective/ > [Accessed on 20.02.2024]
16. Ibid
17. 2017(2) LNJ (HCD) 303
18. Mohammad Shahjahan. Admissibility of Digital Evidence: Bangladesh Perspective, (15 January, 2022), Lawyers Club Bangladesh < http://lawyersclubbangladesh.com/en/2022/01/15/admissibility-of-digitalevidence-bangladesh-perspective/ > [Accessed 20.02.2024]
19. Section 45 was substituted by section 9 of the Evidence (Amendment) Act.2022 (Act No XX of 2022)
20. The Evidence Act, 1872 (I of 1872)
21. Section 45 was substituted by section 9 of the Evidence (Amendment) Act.2022 (Act No XX of 2022)
22. Shweta, Tauseef Ahmad. Relevancy and Admissibility of Digital Evidence: A Comparative Study, IJLMH,2:1:15.
23. Ibid
24. Sections 65A and 65B of The Indian Evidence Act 1872, (Act 1 of 1872)
25. Alex B Makulilo. The admissibility and authentication of digital evidence in Zanzibar under the new Evidence Act, 2018, Digital Evidence and Electronic Signature Law Review [Accessed on 20.02.2024]
26. < https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html#:~:text=Digital%20evidence%20is%20admissible%20if,Justice%2C%202004a%3B%20European%20Network%20of > [Accessed on 20.02.2024]
27. Aida Ashour, Caleb Bowers. An Overview of the Use of Digital Evidence in International Criminal Courts, 2013.
28. Ibid
29. http://dspace.ewubd.edu:8080/bitstream/handle/123456789/3599/Adhora_Ema_Barua.pdf {Chapter 4.2 [Accessed on 20.02.2024]}
30. < https://www.bileta.org.uk/wp-content/uploads/The_Admissibility_and_Authentication_of_Computer_Evidence_-_A_Confusion_of_Issues.pdf >
31. Digital Evidence & the US Criminal Justice System < https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf > [Accessed on 20.02.2024]
32. Ibid
33. Ibid
34. < https://articles.manupatra.com/article-details/ADMISSIBILITY-OF-ELECTRONIC-EVIDENCE-UNDER-THE-INDIAN-EVIDENCE-ACT-1872 > [Accessed on 20.02.2024]
35. Ibid
36. < file:///C:/Users/law/Downloads/6.+Digital+Evidence+and+its+Admissibility+under+Pakistani+Law.pdf > [Accessed on 20.02.2024]