ETHICAL HACKING AND ADMISSIBILITY OF ITS EVIDENCE

Harivignesh.R[1]

JUSTIFICATION FOR THE TOPIC

Computers have become integral part of human activity in home and workplace, most specifically individually use the computer technology for numerous purposes and the business dealings were done in speedy and fast growing manner. Similarly, the digital system nowadays is said to be main stream of line for a criminal activity and one such major crime is *hacking*, which still persists in the cyber world. Even this hacking is used to conceal and remove the evidences from the cyber platform, which creates a new scope for Hacking in an ethical way (i.e., Ethical hacking – Cyber Forensic Investigating) to hack into the cyber platform and retrieve the data which pertain to be an evidence and such data collected should be admissible in the court of law. This project deliberates upon what's ethical hacking (includes the person performing such act), the category of the data that is being collected from the perspective of Evidence and finally the admissibility of such evidences.

RESEARCH OBJECTIVES

- To understand the meaning of the term hacking and its components
- To find-out the legal status of hacking if done with certain ethics
- To examine the procedures to be followed for admissibility of such kind of evidence
- To figure-out the circumstances which portrays hacking as Ethical Hacking.

RESEARCH QUESTIONS

1) Whether Hacking done by any persons other than investigating officers can be considered as Ethical hacking? If not state, the persons if any, authorised to do such act, and the circumstances under which it is considered as ethical Hacking.

[1] 3rd Year B.Com LL.B(Hons) Student, Tamil Nadu National Law School, Tiruchirappalli

2) Whether the Evidence collected by Ethical Hacking is deemed to be, a digital evidence and admissible? If not state, the procedures in which it shall be admissible in court.

HYPOTHESIS

Since, the concept of ethical hacking is per se said to be valid, if it has been done by the forensic investigators or any other person duly authorised by law will be deemed to be admitted as evidence as per section 66 A and 66 B of Indian Evidence Act, 1872. It can determine only on the basic on circumstantial proof which was adduced by the parties to the court. The researcher tries to understand the chronology of events in connection with ethical hacking and tries to put forth the possible outcomes of evidential jurisprudence.

INTRODUCTION

The element of anonymity and lack of territorial borders in cyberspace makes the internet an attractive medium for criminals to commit crimes. Not only the conventional crimes such as thefts, extortion, defamation or forgery are committed through computers but also new forms of crime have emerged such as hacking, Trojan, bot and phishing attacks. Every computer on the internet has an IP address. When a crime is committed, the investigators and law enforcement agencies track the internet protocol address known as IP Address, Media Access Control Number or International Mobile Equipment Identification Number (the IMEI Number) to know form which location, system or device the crime was committed from. With the help of sophisticated software such as Hide IP or use of anonymous proxy servers that allow use of proxy IDs or fake IDs. Cyber criminals flourish in criminal activity on the internet.[2] According to the "P. Ramanatha Aiyar's Advanced Law Lexicon" , the cybercrime generally means & includes ***''Computer Crime committed over the telecommunications networks''- Criminal acts committed by making a computer as a method or means of crime to cause damage to persons and/or property is a cybercrime.***"[3]

Whenever a dispute regarding online contracts or e-crimes is to be adjudicated by a court, production of admissible evidence becomes a focal point of determination of merits of the case.

[2] In a case, use of mobile tower signals pertaining to location of amonile set led to resolving a murder case when an engineer murdered his wife. See PTI, " Bangalore Techie Caught gfor Wife's Murder", Outlookindia.com,14th August, 2010 accessible at http://news.outlookindia.com/item.aspx?690442 (last accessed on 06. 03.2017 at 7.00 pm IST)

[3] See. Seth, K., Computers, Internet & New Technology Laws, 2012.

Certain questions which are important from the perspective of evidence in the offline world are equally important for electronic evidence purposes, including the minimum requirement for admissibility of evidence of an electronic evidence, the onus of proof, the procedural requirements to be fulfilled relating to the examination of electronic evidence, the standards to be adopted while storing, preserving and retrieving electronic evidence.[4] Moreover the IT Act, 2000 in its preamble sets out clearly that its objective is 'to provide legal recognition for transactions carried out by means of data interchange and other means of electronic communication. In accordance with this it provides a legal recognition to electronic records.[5]

Forensics, generally a science to investigate and establish the facts in a criminal or civil court. In the context of cybercrime, the role of computer forensic and digital investigation goes hand in hand, help to acquisition, examination and reporting of information found on computers and other networks that pertain to a criminal or civil investigation. Cyber forensic[6] is increasing for importance for the law enforcement agency for a number of reasons, not the least of which is that computers and the Internet represent the fastest growing technology tools used by criminals and this trend will continue for the foreseeable future.[7] The objective of Computer Forensic Investigator is to determine the nature and events concerning a crime and to locate the perpetrator by following a structured investigative procedure.[8]Cybercrimes and white collar crimes increases day by day, and they are assumed to be an non-violent crimes, yield many more profits, have relatively low risk of capture and if they caught and convicted, usually result in short prison sentences & difficulty in proving with an appropriate evidence.[9]Moreover the IT Act 2000, read with sections 65A and 65B of the Indian Evidence Act, 1872 provides the procedure for proving electronic evidence.[10] The provisions of S.65A elucidate that the

4 *Ibid* at Pg. 409

5 See S.4 Information Technology Act,2000

6 Cyber forensic can be defined as the process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability. The challenge of course is actually finding this data, collecting it, reserving it and presenting it in a manner acceptable in court of law

7 Albert.J.Marcella. Jr.Greenfield, Robert S., Cyber Forensics Available at http://www.cyber-forensicanalysis.com/ Last visited on 06. 03.2017 at 7.00 pm IST

8 Dave Kleiman, The Official CHFI Study Guide (Exam 312-49): for Computer Hacking Forensic Investigator

9 See. Gary.C.Kessler, The Role of Computer Forensics In Law Enforcement, Jan 2006, available at: http//www.officier.com/article/article.jsp?site section=18&id=28161. ,Last visited 06.03.2017 at 7.00 pm IST

10 See sections 65A&B of the Indian Evidence Act, 1872. The Second Schedule of IT Act,2000 provided amendments to the Indian Evidence Act, 1872.

electronic records can be proved in evidence by the parties in accordance with the provisions of S.65B (which will be considered as Secondary evidence.)

The basic purpose of ethical hacker and computer hacking forensic investigator is to keep the important data of business organization or a security agency safe from the malicious hackers. But ethical hackers investigate only the probabilities of hacking a computer system and fix the weakness of the system. The computer hacking forensic investigators, on the other hand, also collect evidences to prosecute the hackers in the court of law along with detecting the reasons of intrusion by the hackers. This project deals with the concept of Hacking and how does it differ from Ethical Hacking moving further with its kinds and the crime it falls under and also the category of evidence and the procedure for admitting the evidence under the Court of Law.

HACKING AND ITS TYPES

"Hacking' means unauthorised access to a computer system. It is the most common type of Cyber Crime being committed across the world. The word 'hacking' has been defined in S.66 of the Information Technology Act, 2000 which means "whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking"[11]

Hackers worldwide attempt to hack into remote computer systems for multiple purposes like data theft, fraud, destruction of data, causing damage to computer systems, or for more pleasure or personal satisfaction. But mere access to any computer resource will not constitute an offence of 'hacking'. In ***DPP v. Bingndl***[12], where two police officers were charged for using the police national computer to gain access to details of motor cars which they wanted for private purposes. They were charged with unauthorised access to computer material. Hacking can be formally defined as either a successful or unsuccessful attempt to gain unauthorized access to a computer system.[13] Hacking as already defined is the unauthorised access to the computer system, which if accessed with proper authorisation is deemed to be Ethical. To

[11] S.66 Information Technology Act, 2000

[12] Micheal P Dierks, Symposium : Electronic Communications and Legal change, Computer Network abuse, 6 Harv. J.L. & Tech.307 n.7 (1993)

[13] Barua Yogesh, Criminal Activities in Cyber World, Dominant Publishers and Distributers, Jan 2005 ,1st Ed.

further deliberate upon the same based on the intent and the kind of act performed the Elite Hackers are classified into 3 *viz.*

- Black Hat Hackers
- White Hat Hackers
- Grey Hat Hackers

Deriving the inference from the name, the classic Black Hat Hackers means the Criminals/ Law breakers and the White Hat Hackers mean the Ethical Hackers who work to protect systems and peoples and finally the Grey Hat Hackers means those persons who dabble in both Black Hat and White Hat tinkering.[14] To quote further *a computer user who willfully vandalizes or commits theft on other people's networks,* which suits for the Black Hat hackers, and the word Black Hat Hackers is one of the illuminate name of describing the persons with malicious motivations. On the other hand, the White Hat Hackers, who are a network specialists employed to help protect computer networks, widely known as the Ethical Hackers. These Ethical Hackers not only be employed for security reasons they also engage in the academic arena to contribute in the creation of clever programs and beautiful interfaces.[15] To mention about the Grey Hat Hackers, it is conflicted and their position is uncertain as to which side of the law they stand. They may act illegally sometimes but usually have good intentions and are usually not motivated by personal gains. The White Hat Hackers is home to security professionals that specialize in penetration testing of systems and other types of do-gooders. These kinds unlike the Black Hat Hackers won't hold the found vulnerabilities they find for extortion purposes, but fully disclose those if any. Mostly the hacking by the White Hat Hacker is pre-authorised by the system owner, prearranged, and within very specific test boundary parameters so that the target's operations aren't damaged or harmed in any way.[16]

But the hackers be it a Ethical Hacker, won't indulge much into the already completed hacking, their main concern is with regard to finding the available vulnerabilities and report to the person who authorised him and in some cases figure out the possible solution to rectify the vulnerability and this job in no way leads to the creation or finding of evidence left behind by the Hackers, which brings in the role of a person to conduct requisite investigation. After the

[14] Paul Gil, What are "Black Hat' an 'White hat' Hackers?, March 21 ,2017 Life Wire https://www.lifewire.com/black-hat-hacker-a-white-hat-hacker-4061415, Last visited 30/03/2017 , 8.00 Pm I.S.T

[15] *Ibid*

[16] Andy O'Donnell, "What Colour is your Hat", August 21,2016 Life Wire, https://www.lifewire.com/what-color-is-your-hacker-hat-2487760, Last visited 30/03/2017 8.15 Pm I.S.T

high-profile data breaches like Sony, Home Depot etc. the demand for well-trained computer Forensic Expert is rising who can conduct the requisite investigation to ascertain the offender and cause of security incident and help to mitigate the damage.[17] The Computer Forensics refers to the process of recovery of the evidence from the computer, laptop and connected devices. Recovery from the file system requires knowledge of various file systems, operating system and every application being used. The Network forensics refers to collecting digital evidence relating to movement of data in the online medium. It is most relevant in today's scenario as the first objective is to trace the origin of data to identify cyber offenders. The Computer forensic professional are referred to by many titles including Computer Forensic Investigator, Digital Media Analysts, Digital Forensic Expert and Digital Forensic Detectives.[18] The forensic expertise are required not just by Law enforcement agencies but also in the corporate world.

DIGITAL EVIDENCE

Digital evidence is any information of probative value that is either stored or transmitted in a digital form and it includes computer evidence, digital audio, digital video, cell phones, digital fax machines, etc. Due to enormous growth in information technology throughout the public & private sector, the evidences which are adduce from electronic form have deemed to be admitted by courts by way of new amendment by virtue of S.92 of the Information Technology Act. Nowadays, the Digital Evidence are mostly relied in civil and criminal cases, Judges often asked for the reliability of such electronic evidence in courts.

In 2000, the Parliament of India enacted the Information Technology (IT) 2000, amending the existing provisions of all Indian Legislation to allow the admissibility of the digital evidence. This new concept of Digital evidence and introduction of the Information Technology Act is based on the United Nations Commission on *International Trade Law Model Law on Electronic Commerce* which leads to the new dimension for the admissibility & creditability of evidence. Certain Indian Legislation like **I**ndian **E**vidence **A**ct 1872, **I**ndian **P**enal **C**ode 1860 and the **B**anker's **B**ook **E**vidence **A**ct 1891 were amendment due to new evolving law

[17] Neeraj Aarira, How to become a Cyber Forensic Examiner, Oct.09,2015, http://www.neerajaarora.com/how-to-become-a-cyber-forensic-examiner/, Last Visited on 31/03/2017 9.00 Am I.S.T

[18] *Ibid*

relating on digital evidence. The various categories of the electronic evidence are as follows : Website data, social network communication, email, SMS/ MMS, and other computer related problems. This part explains about the new amendment of the digital evidence in the Indian legislation most specifically deals with the admissibility of digital evidence in relation with the recent judicial pronouncement.

AMENDMENTS TO INDIAN EVIDENCE ACT

New amendment in the Indian Evidence Act introduces the admissibility of the Digital evidence.

- ***Definition of Evidence was amended*** - Section 3(a) of Indian Evidence Act was amended and the phrase "*All Documents produced for the inspection of the Court"* were substituted by *"All Documents including the "**electronic records**" produced for the inspection of the Court"* -

Form the above definition, it is clear that " Evidence " means and includes two categories:

1. Oral Evidence which consist of statements made by witnesses in the court in relation to the matters of fact under enquiry.
2. Documentary Evidence which consist of documents including ***electronic records*** produced for the inspection of the court.

This term "electronic records" has been given the same meaning as assigned to it in the **IT** Act provides the data which is recorded or generated, image or sound stored received or send in an electronic form. The Delhi High Court in ***Dharambir v. Central Bureau of Investigation***[19] held that, if the electronic device has recorded any data which is relevant for a case, such electronic device shall be treated as electronic record for the purpose of evidence. Section 17 included the statement *"oral or documentary or contained in an electronic form "*which ultimately infers that the Digital form of evidence is deemed to be admissible in courts to frame any fact in issue or form in part of relevant fact. There are certain inclusion of phrases in the Section 39 and amended new section 22A, 65A and 65B in relation with digital evidence.

[19] *Delhi High Court in Dharambir v. Central Bureau of Investigation* 148(2008)DLT 289.

ADMISSIBILITY OF DIGITAL EVIDENCE

Schmidt and Zeffertt expressed the reluctance of the traditional lawyer to welcome to electronic evidence as new species when they stated " in leaving paper, we have also left almost all guarantees of authenticity and reliability.[20]In Rebuttal to this position, Ken Chasse observes:

" The law must reflect the change in technology. Technology changes do not always require changes in the law, but in this case such is necessary. For example, a traditional paper record system gave rise to and therefore can satisfy, the legal concept of an " Original Record". But in electronic record system there is no such thing called "Original"[21]. The printout taken to the court is produced at the end of the record system's function and activities, not at the beginning - not at the acts or events it records, and not by a person having direct personal rule have no electronic counterpart either.. Therefore, a new rule of admissibility is necessary."

The Emergence of the electronically stored Information with the advent of computer science and steady replacement of paper based documents by e-documents, law had to keep a face with technology.[22]Thus, Section 4 & 5 of the IT Act recognised *"Electronic Records"* and Digital Signatures which in turn reflects in Section 3 of Indian Evidence Act. Once the document is recorded digitally, it cannot be " *read"* by a person without using the computer system into which that information was initially fed. It is evident that, the information presented in hard drive is something in the state of original or Primary evidence as per section 62 and it's print out is called as secondary evidence.

India has not abolished the traditional method of paper based documents, but moved towards the permitting proof of e-documents " without further proof or production of Original". Generally the distinction between the primary and secondary evidence gets totally blurred. So, CD will come under the definition of the " *Computer Outputs'* 'being a electronic record as per the Section 65B (1) and treated as a Original Document. Because of unfamiliarity, the courts

[20] Schmidt and Zeffertt, Evidence, para133, Joubert, The Law of South Africa (1997), Vol.9,I st edn., Butterworth's :p.149.

[21] See.Ken chasse, " Electronic Records as Documentary Evidence "., Canadian Journal of Law and Technology., p.156, http://papers.ssrn.com/sol3/papers.cfm?abstract-id=2438350. accessed on 20. 03.2017 at 12.30 PM.

[22] Justice .P.Sathasivam, Judge Supreme Court of India, Speech on " Apprehension of Evidence including Evidence recorded through Electronic media for session cases" at Tamil Nadu State Judicial Academy on 26.03.2011,http://www..hcmadras.tn.nic.in/jacedamy/article/Electronic%20Evidence%20PSJ.Pdf. accessed on 20. 03 .2017 at 2.00 PM.

before took the e-documents as *"real and material evidence"* and now it arrived at the status of "*any other record*." Another issue relating to the application of the best evidence rule to e-evidence is whether it is ***a hearsay evidence***. In the *State v. Armstead*[23], the court held that not all the electronic evidence is the hearsay, as the digital evidence is not the statement by a person but it is an by-product of the machine operation. Electronic Data that is offered for the truth of the matter asserted is typically hearsay and thus generally inadmissible under the evidential rules. To admit the files stored in hardware and the emails as direct evidence, the proponent needs to satisfy the court that it comes from the exception to the hearsay evidence maintained in the ordinary course of business.

INTERPRETATION OF SECTION 65 A & 65B

As per Section 65B, Clause(1) notwithstanding anything contained in the Act, any information contained in an electronic which is printed on paper stored recoded or copied in optical or magnetic media produced by a computer shall be deemed to be a document if the conditions mentioned in Clause (2) are fulfilled and shall be admissible in any proceedings without further proof or production of the original as evidence of any contents of the original or of any fact states therein of which direct evidence would be admissible.

Section 65 B (2) (a) to (d) lays down the conditions to be complied with before the computer output can be considered as document. Clause (3) deal with the tasks of storage or processing of information performed over a period by

a) A combination of computers or
b) Different computers in succession or
c) Different combination of the computer in succession of or
d) Any other manner involving successive operation, in whatever order of one or more computers or one or more combination of computers.

Section 65 B, Clause (4) requires that before any statement is sought to be admitted under the section a certificate must be produced purporting to be signed by person occupying a responsible official position in relation to the operation of the relevant device or the

[23] State v. Armstead, 432 So.2d 837,839(La.1983).

management of the relevant activities identifying the details of the electronic record and the particulars of the device used in the production of the electronic record. The certificate so issued shall be the evidence of any matter stated in the certificate. (In pari materia with section 79A. of the Information of Technology Act, 2008).

Section 64B, clause (4) clarifies the circumstances in which the information shall be taken to have been fed to the computer directly or by means of any equipment with or without human intervention or by another computer.[24]

JUDICIAL CONSTRUCTION

In the case **of *State v. Navjot Sandhu,*[25]** the Supreme Court held that *" the irrespective of the compliance with the requirement of Section 65B* " in the above observation gives the impression that, according to the apex court the electronic evidence will be admissible, even if the certificate which is mandatory under Section 65B(4) is not produced. but the recent case of ***Anvar P.V.v. P.K. Basheer***[26], the SC held that

"The statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this court in Navjot Sandhu case does not lay down the correct legal position. It requires to be overruled and we do so..... It is clarified that notwithstanding what we have stated herein in the preceding paragraphs on the secondary evidence on electronic record with reference to section 59,65A and 65B of the Evidence Act, if an electronic record as such is used as primary evidence under S.62 the same is admissible in evidence without compliance of the condition in Section 65B"

It is evident that U.K, USA and Australia have abolished the traditional best evidence rule as applied to the proof of all documents, India has not abolished the traditional rule with regard to paper based documents but has moved towards permitting proof of e-documents without further proof or production of the original.

[24] Punjab v. Amritsar Beverages Ltd (2006)7 SCC 607: The Apex Court in State v. Navjot Sandhu, (2005)11 SCC 600.
[25] State v. Navjot Sandhu, (2005)11 SCC 600.
[26] Anvar P.V. v.P.K. Basheer and Others. AIR 2015 SC 180.

THE CYBER FORENSIC AND ISSUES IN EVIDENCE

As discussed above, the cyber forensics as scientific knowledge and methods applied of the identification, collection preservation, examination and analysis of information stored or transmitted in a binary or digital form in a computer. The Digital forensic investigator used various methods which may vary based on the case to case, however the process generally includes the planning, and acquisition, and preservation, analysis. Extracting or Presenting the digital evidence is an ultimate challenge for a computer forensic professionals because it determines the relative weight of probative and prejudicial (admissibility) value in the courts. It is the duty of the forensic investigator to introduce the evidence, and consistency in expanding field of extracting and examining evidence. They must be able to retrieve format in as much as analysing the functional details, equipped with forensic tools and the role of each component or any part of the computer involved in the crime. They must also be able to explain in the courts the process involved in the forensic analysis and data retrieval.[27]

The investigators cannot rely upon the raw evidence rather than the standard form of digital evidence. The above said cardinal principal was held in the landmark case called *Cochrane*[28] in which the computer printout obtained from an automated teller machine containing entries in the till rolls was held to be the direct or real evidence of the transactions. The digital forensic investigators and the forensic specialists have to identify the possible sources of the digital evidence including the Hardware components[29], application software, monitoring software, general logs[30] backups & archives and other sources[31]. " An Overview of the Cyber Forensic"

FORENSIC INVESTIGATION

- **Four Important Stages**

  Collection and Preservation of evidence →Extraction of Evidence →Examination of Evidence →Organisation of Evidence.

- **Six Important Process**

[27] Keith J.Jones, Richard Bejtlich and curtis W.Rose, Real Digital Forensics Computer security and incident response, Addison - Wesley Professional: Pap/Cdr edition. October,2005.
[28] R v. Cochrane,1993, United Kingdom
[29] HDD, FDD, Servers, backup & storage devices and other embedded devices.
[30] Access logs, printers logs, web traffic, internet network logs, internet traffic, database transactions and normal business transactions.
[31] Telephone logs .EPBAX data, network records, call centre logs and recorded messages..

Identification → Search and Seizure →Preservation → Examination → Analysis →Reporting

Both the stages and process are mutually inclusive.

Search and Seizure of Digital Evidence is the first process most commonly disputed in all the cases. The issue of search and seizure is closely linked with the issues of privacy also. *Art 12 of UN Declaration of Human Right* ensures the right to privacy to everyone. The citizen have inherent right against the search and seizures which was said to be one of case called *United States v. Triumph Capital Group*[32] case. The use of improper methodology or unlawful search and seizure will have a drastic effect in admissibility of digital evidence. It is the duty of the forensic investigator recognise the limits of the warrants for search and seizure. It leads to an another critical process called **''Evidence Preservation''**[33] which is the paramount duty of the investigator to ensure that the evidence is not destroyed or damaged. The Investigator will have to face several challenges, because the evidence can be manipulated during the collection, analysis and preservation of the evidence and evidence should be protected from virus infection. In *Kucala Enterprises Ltd v. Auto Wax co., Inc*,[34] the lower court was dismissed the case, because the plaintiff did not preserve the evidence but rather destroyed evidence using Evidence Eliminator.

GOOD FAITH AND REASONABLE CARE

The forensic investigator must ensure that all the process and procedures in conducting forensic investigation are within the required legal framework. The investigators must have sound knowledge of legal issues involved in forensic investigations most importantly privacy protection rights & authority for search and seizure of forensic evidence has obtained prior to the investigation. The courts will take into consideration of the fundamental rights of people against unreasonable search and seizure. The forensic investigator have to acted in good faith and took all the reasonable steps in order to preserve the electronic data. It is one of the paramount obligation in which investigator cannot forego at all. If it is destroyed the court may pass some sanction or reparation to the forensic investigator. The above said ruling will

[32] 260 F. Supp 2d 432.

[33] James Tetteh Ami-Narh ,Patricia A.H. Williams : Digital forensics and the legal system: A dilemma of our times : Edith Cowan University,2008.P.4.

[34] 42 F..Supp 2d 821, 833.

expanded to the parties to the dispute also. One example of this is in the case of ***Associates International Inc. v. American Fund ware***[35], the defendant intentionally destroyed the computer code and waive certain duty of preservation in order to escape for liability. In ***Mosaid Tech Inc..v. Samsung Electronics Co***.[36], the defendant was sanctioned by the court, because he/she failed to preserve discoverable evidence that was potential for the dispute and court awarded monetary sanctions for the destruction of evidence.

FORENSIC EXAMINATION & ANALYSIS

The Forensic Investigator must ensure evidential value & evidential integrity of the investigation by imaging an exact copy of all media servers , floppy disk drives, backup tapes, CD ROM's .etc.

In ***Gates Rubber Co. Bando Chemical Industry***[37], the court awarded the sanctions and criticized the experts for not making an image copy of the drive at issue. The Court discussed the mirror imaging process, the authenticity of data taken from the image and admitted the evidence. The rules of evidence which determines the admissibility of findings in the court of law and courts demands certain proper procedural fairness i.e. the proper analysis have to be done and the accuracy of methods which are used to find evidence, that should not be tampered within the process of analysis. The Forensic investigator should be able to defend forensic finding in the courts and also improper analysis of evidence can adversely affects the creditability of the evidence. The testimony of the computer forensic expert is always challenged in the courts because of his good educational background, skill, knowledge and experience, the above argument stands defeated.

[35] 831 F. Supp .1516 (1993)
[36] 362 F.2d 526.
[37] 167 F.R. D.90: 1996.

CONCLUSION AND RECOMMENDATIONS

Computer Security is a very hot topic these days. There are a lot of jobs available on both sides of the line. There is a new breed of hacker, The Criminal Hacker, to break into computer systems, and cracking code, not out of curiosity, but out of greed. So, there is a definite need to protect data from unauthorized access. Programmers are often called upon to provide for secure access to data, which already discussed as given by the Ethical Hackers. After further deliberation into the work of the Ethical hacker, it is clear as to the work of the so-called person who is termed as an Ethical Hacker is slightly different from that of the Forensic Investigator. The simple meaning of computer forensic is the application of the techniques of computer investigation and analysis to determine the potential legal evidences for the safety of the computer system of the organisation in future. These evidences can be required to resolve a number of computer related misuse or crimes along with theft or damage of intellectual property, frauds and theft of trade secrets etc. But still there is a slight confusion as to whether the Forensic investigator come under the purview of Ethical Hacking. But as of now the evidence produced by the Forensic Investigator is deemed to be admissible before the court of law. But the position of an ethical hacker being working under any of the Government department is still not clear and so the admissibility of the evidence collected by such persons is also not clear. Moreover, since the opinion of the Forensic Investigator is considered as an expert opinion, will the opinion of an ethical hacker also be given such value? These are the questions that still prevail and which has to be deliberated upon further to clear off the mirage that prevails. From the above analysis, this cyber world created a new dimension for the forensic investigator to perform their duties with the help of forensic methods & forensic tools and techniques. The Forensic investigator faces the various problem in conducting forensic investigation and presenting forensic evidence before the court, and these evidences provided are said to deem to be admissible. This Paper clearly explains about the stages and process of the presenting the digital evidence and visualises the practical difficulty in presenting it. The paper further explain about the digital evidence which are presented before the court must be satisfied the condition and procedures prescribed in the S.65B of the IEA or else it does not claim to be an evidence at all, before the court of law.