Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 7, July 2020, pg.86 – 89

Legal Issues in Computer Forensics and Digital Evidence Admissibility

George Raburu[1]; Lawrence Dinga[2]

[1]School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, P. O. Box 210- 40601, Bondo, Kenya. graburu@jooust.ac.ke

[2]Management Systems Limited, P.O. Box 39362, Nairobi, Kenya ldinga@managecom.co.ke

ABSTRACT: ***COMPUTER FORENSICS INTEGRATES THE FIELDS OF COMPUTER SCIENCE AND LAW TO INVESTIGATE CRIME. FOR DIGITAL EVIDENCE TO BE LEGALLY ADMISSIBLE IN COURT, INVESTIGATORS SHOULD FOLLOW PROPER LEGAL PROCEDURES WHEN RECOVERING AND ANALYZING DATA FROM COMPUTER SYSTEMS. THE LAWS WRITTEN BEFORE THE ERA OF COMPUTER FORENSICS ARE OFTEN OUTDATED AND CANNOT ADEQUATELY ASSESS THE TECHNIQUES USED IN A COMPUTER SYSTEM SEARCH. THE INABILITY OF THE LAW TO KEEP PACE WITH TECHNOLOGICAL ADVANCEMENTS MAY ULTIMATELY LIMIT THE USE OF COMPUTER FORENSICS EVIDENCE IN COURT. THIS PAPER DISCUSSES LEGAL ISSUES IN COMPUTER FORENSICS INVESTIGATIONS PROCESS AND ADMISSIBILITY OF DIGITAL EVIDENCE IN COURT OF LAW.***

KEYWORDS: FORENSICS, ADMISSIBILITY, DIGITAL EVIDENCE, JURISDICTION, LITIGATION

1. Introduction

Computer forensics is a branch of forensic science that involves methodical application of computer investigation and analysis techniques to gather evidence found in computers and digital storage media. Computer forensics involves the use of sophisticated and modern technology tools and procedures to identify, preserve, recover, analyze and present digital evidence in a manner that is legally admissible in a court of law. In short, computer forensics is the convergence of science and law. This means computer forensics investigations should follow defined procedures that take into account industry and organizational practices as well as appropriate laws. Given that many legal systems worldwide are based on precedents, computer forensics investigators apply cohesive and consistent procedures in extracting and examining digital evidence in order to avoid legal challenges when presenting that evidence in court of law.

2. Case Jurisdiction

In many legal systems around the world, courts can only adjudicate cases that fall within their jurisdictions. In cases involving computer forensics, the jurisdiction of the cybercrime perpetrator may differ from the one where data and information is located. Digital evidence must therefore satisfy the expected legal rules of evidence in a particular jurisdiction in order to be legally admissible. This poses another problem because an operation that constitutes an offence in one jurisdiction might not be actionable in another jurisdiction if it is not defined within its laws. In *Dow Jones & Company Inc v Gutnick*, the Australia's High Court ruled that in defamation cases, an article posted on the internet is considered as published at the point where it is downloaded and read and awarded an Australian

businessman the right to sue for defamation in Australia over an article published in the United States and posted on the Internet.

In *Braintech v Kostiuk*, the Supreme Court of Canada held that information presented in the internet and accessed by users in overseas countries cannot warrant adequate grounds to grant a court in a different country to establish its authority and held that the Texas Court lacked the sovereignty over an inhabitant of British Columbia.

3. Search and Seizure of Digital Evidence

Search and seizure is often a target of contestation in court since it is synonymously associated to the question of privacy. Privacy laws in many countries including article 12 of the UN Declaration on Human recognizes the right of privacy which protects people from unnecessary searches and seizures. In computer forensics investigation, search and seizure is the initial process and therefore use of improper methodology has a potential negative impact on the admissibility of the evidence. Forensic investigators are therefore obligated not to infringe the privacy of the suspect in the course of their searching and ensure that proper legal procedure is followed in addition to a search warrant. However, forensic searches and seizures often differ from the traditional methods of searches. The traditional methods of searches do not take into consideration technological advancements which make the search warrants inadequately detailed when being executed. For instance, in situations where a forensic investigator armed with a warrant to seize a computer and finds that the suspect's data is located in the clouds. It will be impossible to retrieve the required evidence. In some instances, the investigator may find that the computer to be seized as per the search warrant is a server running RAID technology. Not only will it be impossible to seize the server but also different technology will have to be used to retrieve data.

The forensic investigator must identify and articulate the reasons for obtaining search warrant and recognize the limits of such warrants. In many jurisdictions, search warrants must be very clear on what to search and seize. This poses a problem with digital evidence in cases where the investigator comes across incriminating evidence in plain view but not covered by the search warrant such as child pornography. In this case there is risk of the new evidence being hidden, altered or destroyed before a new search warrant is issued. Speed must be of essence if the new evidence has to be brought to court. In *Wisconsin v Schroeder,* the court issued the investigating officer with a search warrant to confiscate the suspect's computer and its accessories in a case involving online harassment. During the search process, the investigator came across some child pornographic images and the process was stopped and additional search warrant was sought to give the investigating officer the power to search for child pornographic images.

4. Evidence Preservation and Spoliation

The nature of digital evidence is that it is generally fragile and can easily lose its value not collected, preserved, and guarded in a proper and timely manner. It can be effortlessly erased or modified by just a simple click. Therefore it is essential that evidence preservation is addressed in the early stages of investigation. The investigating officer must be able to demonstrate in court that the evidence was not altered in any way and can be trusted to be truthful in order to be admissible. This can be established through a chain of custody which is a documentation that shows how the evidence was collected, preserved, analyzed and eventually presented in the court of law. A clear chain of custody demonstrates that the evidence is trustworthy. In many jurisdictions, existing legal procedures are inadequate to address the preservation of digital evidence in litigation cases and the investigators lack the required training and technical knowhow to implement chain of custody procedures. The electronic discovery processes and technologies involved are often seen as expensive and current procedures mostly address only preservation of manual paper documents. In *Weiller v New York Life Insurance Company*, the defendant was ordered to preserve documents but maintained that it would be very expensive to preserve computer information. It was held by the New York court that the federal preservation orders did not provide adequate protection to the plaintiff.

Individuals and organizations often destroy documents during day to day running of business and lack of e-discovery policies in many organizations render preservation of data and electronically stored

information very difficult. Furthermore courts are still reluctant to recognize and expand the litigation process to include electronic data.

5. Examination of Evidence

For digital evidence to be admissible, the forensic investigator must ensure its authenticity and integrity by making bit stream copy of the original media using appropriate forensic software. Under no circumstances should the investigator analyze the original media as this is supposed to be produced in court as exhibit or in case the opposing side disputes the results. Mirror image is used as a means of preserving the evidentiary value of the information recovered. Even though there is possibility to tamper with digital evidence, proper forensic process can unveil this deliberate fabrication. In *State v Cook*, the defendant petitioned against a ruling for the ownership and custody of child pornography. However, the defendant insisted that portions of admitted evidence by the prosecution were not mirrored images produced from his hard disk. The court then debated the forensic imaging procedures, the originality of imaged data, and the possibility of evidence tampering and the appellate court upheld the trial court decision that the evidence was admissible

In *United States v Jackson*, the defendant filed a submission to expunge evidence of chat room discussions arguing that some parts of the transcript had been excluded. There were many errors because the investigator captured the evidence using cut and paste procedure making several parts of the discussion thread being excluded. It was held by the court that cut and paste was not authentic procedure and the evidence was not credible and therefore inadmissible.

Digital evidence admissibility in the court of law is governed by evidence rules that demonstrate the validity of the process used to acquire the said evidence and proof that it has not been interfered with in any way. Many jurisdictions have rules of evidence that inadequately address the processes of validating digital evidence.

6. Evidence Analysis

Improper analysis of evidence can have adverse impact on its admissibility in court of law. It is the responsibility of the forensic investigating officer to convince the court and attest to the credibility of his evidence through expert testimony. To establish credibility and authenticity of the evidence, the investigating officer will have to attest as to the kind of forensic training they have gone through, the investigation skills that they employed, the tools they used to acquire or analyze the said evidence, and the process they used to preserve the digital evidence in preparation for presentation in court.

In *Galaxy Computer Services Inc. v Baker*, the experience and training of computer forensic expert was challenged. The defendant argued that computer expert did not possess the right qualifications and his investigating procedures were doubtful and therefore his testimony should be excluded. However the court rejected the argument and stated that the expert possessed good education and had appropriate skills, knowledge and requisite experience.

In *Peach v Bird*, the defendant who had in his custody child pornographic images was first acquitted of the charge since evidence analysis from his computer failed to link him to the child pornographic websites. On appeal, the plaintiff based his argument on the use Encase evidence analysis and forensic expert testimony. The appellant court overturned the dismissal and ordered fresh retrial.

Many jurisdictions still do not have laws or standards for expert qualifications and the question arises on whether to consider one as expert based on the ability to use forensic software tool or not.

7. Conclusion

Computer forensics investigations help identify, preserve and extract computer and other digital evidence. However, there are significant legal issues that investigators should deal with. Failure to observe due care and attention to the legal rules surrounding the collection and uses of digital evidence can not only make the evidence worthless and being ruled inadmissible in court, it can leave investigators vulnerable to liability in countersuits and evidence.

Many countries, however, have not updated their laws to cater for admission of digital evidence in courts. Existing legislations need to be updated regularly to cater for the emerging changes in new technology and ones enacted to address this gap as well as training judicial and law enforcement personnel who are charged with adjudicating cases in which digital evidence is involved. Training should entail both basic and technical aspects.

References

[1]. ANGELA, B., & RODGER, J. (2005). Identification of legal issues for computer forensics. *Information Systems Management*. Accessed 03 January 2018.

[2]. ALLEN, W. (2005). Computer forensics. *Security & Privacy, IEEE, 3*(4), 59-62.

[3]. BAGGILI, M. *Search and Seizure from a Digital Perspective: A reflection on Kerr's Harvard Law.* http://www.forensicfocus.com/search-and-seizure-digital-perspective Accessed 02 January 2018.

[4]. DEAN, B. (2007). *Knoxville's E-Discovery Newsletter* http://www.forensicdiscoveries.com/previousnewsletters/September_EDiscovery_Newsletter.pdf. Accessed 02 January 2018.

[5]. JAMES,T., & PATRICIA, A.H. (2008). Digital forensics and the legal system: A dilemma of our times. Edith Cowan University, Research Online http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf Accessed 03 January 2018.

[6]. KROLLONTRACK INC. (2004). *Cyber Crime & Computer Forensics News.* http://www.krollontrack.com/newsletters/Cybercrime/oct04.html Accessed 02 January 2018.

[7]. KROLLONTRACK INC. (2006). *Cyber Crime and Computer Forensics News*. http://www.krollontrack.com/newsletters/cybercrime/dec07.html Accessed 02 January 2018.

[8]. MCCONCHIE LAW CORPORATION (1999). http://www.libelandprivacy.com/cyberlibel_docs/Braintech.html Accessed 01 January 2018.

[9]. MELBOURNE JOURNAL OF LAW (2002) http://law.unimelb.edu.au/__data/assets/pdf_file/0007/1680343/Garnett.pdf

[10]. PARTZAKIS, J., & LIMONGELI, V. (2003). *Evidentiary authentication within the Encase*. http://www1.stpt.usf.edu/gkearns/ArticlesFraud/EEEauthentication.pdf. Accessed 01 January 2018 Accessed 02 January 2018.

[11]. OUT-LAW.COM News. (2002). Australia rules on where to sue for internet defamation. https://www.out-law.com/page-3184 Accessed 01 January 2018.

