International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Digital Forensics: Legality of the Process in Cameroon

Joan B.Ali*

Computer science Department, Faculty of Science, University of Buea P.0 Box 63 Buea, Cameroon
Email: ajoanberi@gmail.com

Abstract

In many legal systems today, it is important for evidence that is obtained for use in any judicial proceedings, especially criminal and civil prosecutions, to be obtained lawfully. In other words, evidence should be obtained and examined in such a way as to make it relied upon in court. Part III of the 2010 LAW N° 2010/012 OF 21 DECEMBER 2010, law relating to cyber security and cyber criminality in Cameroon creates a procedural law provision to punish criminal offence of cyber criminality, which has a significance on the acquisition, examination, and analysis of digital evidence; knowing that traditional digital forensic processes, most be legally authorized, so that they do not potentially contravene this law. Cameroon is faced with constraints and limitations in the way digital evidence is interpreted and handled in the courts. These constraints are related to skills, time, laws, technology and cost. The huge limitation is the lack of experts with appropriate skills to carry out digital forensic processes. The legal implications and ramifications for both digital forensics experts, law enforcement, and the cases that they are engaged in are identified, and provide appropriate legal solutions to ensure that these digital forensic practitioners do not contravene the existing laws.

Keywords: digital Forensics; digital evidence; cyber criminality.

1. Introduction

Digital evidence has become a fundamental part of many investigations given the widespread use of digital devices in today's businesses. Digital evidence has been defined as information of a probative value that is either stored, or transmitted in a digital format, in a legal context [1]. The proliferation of digital devices and their use in information communication and the Internet means that digital evidence can be present in virtually any case that involve physical and digital crime scene, and not limited only to computer crimes as was the case earlier in the decade. It has become relevant to the investigation of almost any crime given today scenario [2].

---

* Corresponding author.
E-mail address: ajoanberi@gmail.com.

Almost all the cases investigated by the Federal Bureau of Investigation (FBI) use some type of digital evidence. In the United States of America, the use of digital evidence in court is frequent and cases are decided based on digital evidence [3]. While no such definitive evidence exists in the Cameroon courts, observations made by the researcher support the assertion that more and more crimes in Cameroon are dependent on digital evidence of one form or another. Given the remarkable improvement in the penetration of the use of ICTs; the Mobile telephone penetration year end 2015 stands at 84%, fixed/fixed-wireless at 5% and internet 7% this is a remarkable improvement from past years [6]. The recent award in Cameroon of licenses to mobile operators to operator on the 3G platform which will witness an increase in online activities [7].

It is important to ensure that the admissibility of digital evidence involve processes based on the practices of criminalistics and digital forensic science. In relation to digital evidence, digital forensics is a critical component in bringing evidence to court, as the use of digital forensics follows certain standard processes and procedures which tend to persuade the court to admit digital evidence and give due and proper evidential weight to it [5]. As digital forensics is a specialized field, the courts in Cameroon have tended to treat evidence presented as a result of a digital forensic process as expert witness evidence. As persons who are considered by the courts as experts, they must be held to the standard of an expert, especially within a legal context. As experts in the field of digital forensics, digital forensic practitioners are expected to have a good understanding of the laws applicable to themselves and their field.

In the field of digital forensics, Part III of the 2010 LAW N° 2010/012 OF 21 DECEMBER 2010, law relating to cyber security and cyber criminality is a crucial piece of legislation that digital forensic practitioners need to know and understand failure to understand the offences contained in it could impact negatively on digital evidence presented in court [14].

2. Presentation of Digital Evidence

A trial involving digital evidence may differ fundamentally from other trials in two ways. First, legal issues relating to the admissibility of digital evidence will nearly always arise in the court room. This will include firstly issues like Courtroom Preparation and Evidence Rules that will need to be addressed, secondly, a trial involving digital evidence may involve complex and unfamiliar terms, issues, and concepts. To successfully present a case involving digital evidence the follow are required:

2.1 Educating the audience

If a case is complex, educate the audience, both the judge and the jury at every stage of the litigation process. Such education should address the following:

A. Daubert Test and Pretrial Hearings

This includes the relevance and reliability which requires the judge trying the case ensures that the expert's testimony is relevant to the case and that it rests on a reliable foundation based on Scientific knowledge, that is scientific method/methodology which is conclusion that will qualify as scientific knowledge if the proponent

can demonstrate that it is the results of a sound scientific methodology derived from sound scientific method.

B. Voir Dire

This is a legal variety of procedures connected with jury trials, involving an oath taken by jurors to tell the truth, i.e., to say what is true, what is objectively accurate or subjectively honest, or both.

C. Opening Statement

Opening statement most straight to the point, simple and clear to understand. Most be stated such that it set the stage for evidence presentation.

D. Witness Testimony

Witnesses but be knowledgeable in all the evidence gathered and should be able to present their evidence in a way the judges and jury can understand.

E. Making and Answering Objections

Objection of digital evidence most be technically proven if need be.

F. Closing

Closing should make the case for integrity and reliability.

Most cases in Cameroon, require that the practitioners educate audience to get up to a minimum level of competency and understanding of some basic concepts in information technology so that they can better understand the evidence. Do not make the audience experts because this is why experts are for. It is required that prosecution is kept simple as a general rule, and that holds true especially in the presentation of a digital crime case that is complex by nature that is always the case with digital evidence. Let the defense make things complex prosecution should not. Consider which issues will be hand

2.2 Need to be proved/disproved certain evidence

Most digital evidence cases in Cameroon require a determination by the prosecutor of what should be kept out of digital evidence in a digital crime case. The key evidence are: Is it necessary to disprove all alternative claims and explanations? Can all reasonable alternative explanations be disproved? Some of the aspects to consider are;

A. Technical Anomalies

The nature of computer incidents means that in some instances there will be no complete or clearly adequate explanation for a particular anomaly in the evidence. For example the existence of unexplained bugs or glitches that could create doubts in the validity of data and information stored or processed by a computer is cleared.

Often there will be a conflict between the practical limits on what one wants to or can prove or disprove and often may lead to defense attorney's use of alternative explanations to create reasonable doubt.

B. Disproving Alternatives

What a prosecutor has to disprove depends on the issues involved in a case and the strength of the whole the case. When a crucial element of a case is knowledge (e.g., in a possession of child pornography images case), the prosecutor must be prepared to disprove defense possible claims that the pornography images were stored on the defendant's computer without his knowledge. The prosecutor does not need to disprove unreasonable alternatives (e.g., that the images appeared on the defendant's computer out of the ether).

When the hash values are different between the original evidence and the forensic copy, but there is an overwhelming amount of evidence on the computer (e.g., thousands of child porn pictures) the discrepancy in the hash values can be described and argued as irrelevant to the real issues in the case.

C. 'Timing is everything'

When to rebut a defense is important. For example, if the defendant's knowledge of the contents of her/his computer will be crucial, it is wise sometimes to let the defendant raise the issue about this and allow the evidence (either through cross examination or rebuttal) rebut this claim, rather than asserting to state this during the main proceedings. Some judges will often attach more importance to issues raised in the case as stated, and will believe more in the prosecutor version than when the defense has raised the issue and the prosecutor is merely attacking the defense argument which is usually led during case-in-chief and this objections and argument save for cross examination.

2.3 Expert Witnesses/Scientific Method Evidence needed

Some major decisions in cases that involve complex technology and in need of extensive forensic examination of the digital evidence is whether to use an expert witness (qualified person by special training, knowledge, or experience, in the area to give an opinion). A witness can testify to extremely complex case without having to qualify as an expert witness or be asked to give an expert opinion about a particular event. Some examples are;

Example 1: In many cases involving digital evidence, either the investigator at the crime scene or an expert forensic examiner can testify as to how digital evidence was located and retrieved. While the forensic examination process involve a scientific method, the examiner may have used expert's skills and techniques to collect evidence, but the relevant issue at trial will be whether the evidence in question was on the suspect's device, and not how it was located. The issue here will be either the evidence is or is not on the device. For this, the examiner is a fact witness. Even if a scientific method was used to locate or identify evidence, unless an expert is giving an opinion based on that scientific method, the method does not have to meet the *Daubert standard* relating to Integrity, Discovery, and Disclosure of Electronic Evidence.

Example 2: If a metal detector is used to detect spent cartridges at a crime scene, there is no need to qualify the 'science' of metal detectors to testify. Once the cartridge is found the issue focuses on the cartridge and the only expert witness would be a ballistic expert. Most cases involving digital evidence should be viewed similarly.

3. The digital forensics process

Digital forensics is the collection, preservation, identification, extraction, analyzing and documentation of digital evidence stored as data. Essentially, digital forensics is about evidence from computer, digital media, or digital devices which can stand up to scrutiny in court and be convincing [8]. The objectives being to recover, analyze, and present digital evidence in such a way that it is acceptable as evidence in a court of law. One of the many definitions of digital forensics is that it is the science of acquiring, preserving, retrieving, analysing and presenting data that has been electronically processed and stored on digital media [2]. In some cases, digital forensics is considered to be investigation and analysis techniques that involve the identification, preservation, extraction, analysis, documentation, and interpretation of electronic data to determine any potential legal evidence [9]. Digital forensics also involves the application of science and engineering to the legal problems associated with digital evidence, it is a synthesis of science and the law [10]. Process of digital forensics are used to scientifically derive and prove methods used in the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources. These may be used for the purpose of facilitating or furthering the reconstruction of events of a crime scene or an incident that led to a crime, or helping to anticipate unauthorised actions and digital misuse [11].

3.1 Digital Evidence

Evidence is known as anything that tend to logically prove or disprove a fact of an issue in a judicial case [2]. Digital evidence is defined as information of a legal probative value that is either stored, or transmitted in a digital form [1]. Other definition for digital evidence is that it is any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred, or can address a critical element such as intention or an alibi [1]. Digital evidence is fundamentally no more than digital data found on digital devices. These devices must be capable of storing data.

3.2 Digital Forensic Models

Digital forensics is process, with defined stages, this stages are crucial in that digital forensics need to be understood within that context of its use as well. A number of models have been proposed that describe the various stages within this process. The basic digital forensics methodology is [12]:

- Acquiring the evidence without altering or damaging the source.
- Authenticating that the evidence that you have collected is exactly the same as the source from which it was made.
- Analyze the evidence without altering it. Another model of the digital forensic process includes the following stages [1]:

- Authorisation and Preparation.
- Identification.
- Documentation, Collection, and Preservation.
- Examination and Analysis.
- Reconstruction.
- Reporting Results.

Based on the various models, the common digital forensic process includes acquiring the digital evidence, examining the digital evidence, and analyzing the digital evidence and reporting the findings.

4. Digital forensics and the 2010 LAW N° 2010/012 OF 21 DECEMBER 2010,

This is the law relating to cyber security and cyber criminality, and the fundamental offense defined by the law [14], is when anyone accesses any data without authorization or permission. Considering that the essential digital forensic processes require a digital forensic practitioner to access data, and that this access as a fundamental part of the digital forensics process is always intentional; if this access occurs without the appropriate permission or authorization, then they commit a criminal offence. In other words, if any digital forensics process is performed in relation to any data (including forensic acquisition and imaging, examination, and analysis), and that they did not have permission or authority from an appropriate person or authority to do so; then they have contravened of this law, and could potentially be prosecuted and convicted.

5. The necessity for legality in conducting digital forensics

For evidence to be useable in any court proceedings, it must be admissible. If it is not admissible, then in may not be considered in the case before court, as it may unfairly prejudice or give an unfair advantage to one of the parties of the court case. In addition to the legal requirements and rules which governed the use of digital evidence in court, traditional concepts in the law of evidence nevertheless still apply.

5.1 Admissibility of digital evidence

The Admissibility of Digital Evidence Obtained by applying the procedures of Part III of the 2010 LAW N° 2010/012 OF 21 DECEMBER 2010, law relating to cyber security and cyber criminality Evidence is either admissible or inadmissible [9]. Admissible evidence is evidence that meets all regulatory and statutory requirements, and has been correctly obtained and handled. The quickest methods to ensure that evidence will not be admissible in court would be to collect it in an illegal manner [9], or to obtain it without the correct authorisation [1]. The law in Cameroon has placed a duty on the courts to rule evidence as inadmissible if it was obtained in violation of any aspects of the law and if its admission would result in an unfair trial or be detrimental to the administration of justice. In general in Cameroon, evidence that has been obtained unlawfully, that is in contravention of the law, then it would probably be ruled inadmissible in a criminal prosecution, and may potentially be ruled inadmissible in civil proceedings as well [15]. The key issue is whether or not allowing evidence that had been obtained unlawfully would render the trial unfair or be

detrimental to the administration of justice [9]. Essentially this means that if the digital evidence has been obtained in contravention of the law on cyber criminality in Cameroon, then there is a real probability that it could be ruled inadmissible in a court of law. To insure that digital evidence is not at risk of being ruled inadmissible, it must be obtained legally, and as such digital forensic practitioners should ensure that they do not contravene Sections that address that in the law, and thus there is a necessity to have the appropriate legal authority to conduct digital forensics.

5.2 Avoiding Criminal and Civil Liability

Beside the necessity for legal authority when conducting digital forensics to ensure that the digital evidence will be admissible and thus usable in a court of law, the other necessity for ensuring legal authority is to prevent criminal and civil liability by the digital forensic practitioner. If a digital forensic examiner does not have the appropriate authority or permission to access the data necessary for the digital forensic process, and they do so, then they face the risk of being criminally prosecuted in terms of the law, which carries the possibility of a various fines or imprisonment [13], but the digital forensic practitioner could potentially be subject to civil litigation for delict.

6. Obtaining legal authority

To be able to conduct digital forensics, a digital forensics practitioner requires access to the data that they will conduct digital forensics processes on. This generally requires access to the physical electronic device or storage media containing the data, and the authority or permission to access these and thus the data contained thereon. There is one method to obtain the necessary legal authority to gain access to the physical electronic devices and storage media which contain data which is necessary for digital forensic processes. This is by requisition from a legal authority in Cameroon charged with the competence of judicial investigations [13].

6.1 Digital Evidence in Cameroon

Cameroon has 12 Appeal courts, 46 high courts and 29 courts of first Instance. There courts are distributed over the ten regions of Cameroon with at least one appeal court and high courts in each region [14]. None of these use multimedia facilities in court proceedings. The concept of digital evidence is new and very few trained judges and law enforcement together with prosecutors have the skills to interpret digital evidence. Every day the courts are faced with criminal cases that have components including digital evidence. In most of these cases suspects would have used digital device like the mobile or smart phone in communication. Most of the time this will involve mobile forensic tools to collect and analyses evidence. In Cameroon digital images cannot be admitted in evidence because the judges cannot authenticate them, they still demand the traditional photography method of using picture negatives as a source of evidence. Emails are admitted by using print which usually are not reliable and cannot stand the proof of authentication. Judges have very little technical skills, and will hardly understand most technical terms. 99% of the court system have limited knowledge of digital evidence and hence difficulty in its use.

With the recent advancement in technology and the penetration rate of IT and mobile use increasing it is a big

challenge for the country to properly persecute cybercrimes. The need to help the legal system understand the procedures and challenges involved in the prosecution of digital evidence. In Cameroon digital evidence is mostly for criminal cases

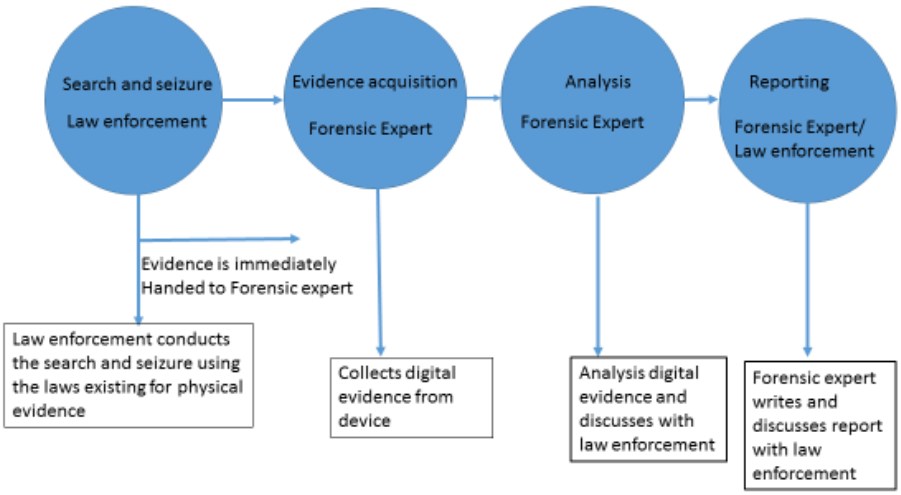

Figure 1: the process used in digital forensic investigation process in Cameroon

In these cases the lead investigator is law enforcement, and most of the time expert witness has hardly testified, expert reports are submitted and interpreted by the legal authorities. Figure 1 above shows the process used in digital forensic investigation process in Cameroon.

The problem with this process is that the law enforcement officers do not understand the basic processes involved in the digital forensic procedure. While the concept is new many prosecutors have prosecuted cybercrime like traditional crimes and digital evidence treated as such. For example cases involving emails are not authenticated and any printout as long as it has an address corresponding is admitted as evidence.

7. Conclusion and Recommendations

The legality of digital forensics and the use of resulting digital evidence in the court room in Cameroon is new and has many challenges. Some of these challenges are as a result of lack of skills from all key players. It is therefore important to train law enforcement on the concept of digital evidence and how it should be presented in the court room. All the process involved in the handling of digital evidence most be followed and guideline to using the present law in digital forensic process be made clearer to both investigators, law enforcement and prosecutors. This way investigators and law enforcement would do the necessary to provide integrity and digital evidence that can be authenticated.

The digital forensic process, unless performed on data that has been obtained with the appropriate legal authorization, satisfies the entire element necessary in the 2010 law on cyber security and cyber criminality in Cameroon. This could result in digital evidence obtained as a result of these digital forensic processes being ruled inadmissible, or even potentially worse, the digital forensic practitioners involved being prosecuted or litigated against. To ensure the legality of the digital forensic process, a key issue is to ensure that before any digital forensic processes are conducted on any data that the appropriate legal authority is in place.

The recommendations following this study are that both judiciary and law enforcement should acquire basic skills to be able to identify and understand the concepts and procedures required in digital forensic process, the attributes and properties of digital evidence to effectively handle digital evidence in the court room. The laws relating to cyber criminality should be revised to reflect the difference that exists between digital evidence and physical evidence. Digital forensic experts should be able to collect and analyze digital evidence following acceptable procedures but at the same time interpreting the laws of the country.

References

[1] Casey, E, (2004), *Digital Evidence and Computer Crime*, 2nd ed. London: Academic Press.

[2] Swanson, C R, Chamelin, N C, Territo, L, & Taylor, R W, (2006), *Criminal Investigation*, 9th ed. New York: McGraw-Hill.

[3] Peisert, S, Sishop, M, & Marzullo, K, (2008), "Computer Forensics in Forensics," in *Systematic Approaches to Digital Forensic Engineering*, pp. 102122.

[4] Van Der Merwe, D, Roos, A, Pistorius, T, & Eiselen, S, (2008), *Information and Communications Technology Law*. Durban: Lexis Nexis.

[5] Carrier, Brian, and Eugene H. Spafford. "Getting physical with the digital investigation process." *International Journal of digital evidence* 2.2 (2003): 1-20.

[6] Website: http://www.budde.com.au/Research/Cameroon-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses.html, last date accessed 4\4\2015.

[7] Website: http://crtv.cm/fr/latest-news/science-et-technologie-9/third-generation-3g-network-cameroon-to-renew-mtn-mobile-licence-14216.htm, last date accessed 4\4\2015.

[8] Vacca, J R, (2005), *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. Boston: Thomson.

[9] Solomon, M G, Barrett, D, & Broom, N, (2005,) *Computer Forensics Jump Start*. Alameda: Sybex.

[10] Jones, A & Valli, C, (2009,) *Building a Digital Forensic Laboratory*. Burlington: Syngress.

[11] McKemmish, R, (2008), "When is Digital Evidence Forensically Sound?," in *Advances in Digital*

Forensics IV, Indrajit Ray and Sujeet Shenoi, Eds. Boston:Springer, pp. 3-15.

[12] Sansurooah, K, (2006), "Taxonomy of Computer Forensics Methodologies and Procedures for Digital Evidence Seizure," in *Proceedings of the 4th Australian Digital Forensics Conference*, Perth, pp. 67-77.

[13] http://fakoamerica.typepad.com/files/law_relating_to_cybersecurity_and_cybercriminality-1.pdf, date downloaded 4\4\2015..

[14] http://www.justiceandpeacebamenda.org/attachments/article/24/The+Judicial+System+in+Cameroon.pdf, date downloaded 4\4\2015.

[15] http://www.crc.bg/files/_en/ZES_ENG.pdf, date downloaded 4\4\2015.

[16] Giannelli & E. Imwinkelried, Scientific Evidence §§ 1.06, 1.16 (4th ed. 2007)