THE INTRICACIES OF DIGITAL FORENSICS: A LEGAL POINT OF VIEW

Written by ***Edie Diabe Pascal***

Senior lecturer at the University of Douala-Cameroon, Faculty of Law and Political Science, Department of English Law, Cameroon

ABSTRACT

Digital forensics refers to the process of retrieval, preservation, analysis, and presentation of electronic evidence for use in investigations and prosecutions of various forms of crime, including cybercrime. Cybercriminals wreak havoc in a multitude of ways identity theft, cyberbullying, data leakage, distributed denials of service, and malware attacks on medical devices and smart vehicles. They stand ready to bring businesses and governments to their knees. Cyberattacks can have a significant socioeconomic impact on both global enterprises and individuals. Therefore, cybercriminals should be promptly identified, and high-quality evidences of the attacks should be made available in the courtroom. This paper provides an overview of digital forensics and electronic evidence, looking in particular at the digital forensics process, common digital forensics practices, standards for digital forensics and electronic evidence, and best practices in digital forensics globally[i]with some emphasis on Cameroon.

Keywords**:** Digital forensics, Investigation, Digital Devices, Evidence, Process Models, Cybercrime, Prioritisation, Data Reduction and Data Mining Framework

INTRODUCTION

The field of digital forensics has become commonplace due to the increasing prevalence of technology since the late 20th century, and the inevitable relevance of this technology in the conducting of criminal activity. In traditional forensics, the evidence is generally something tangible that could identify the criminal, such as hair, blood or fingerprints. In contrast, digital forensics deals with files and data in digital form extracted from digital devices. Digital forensics is a widely-used term, referring to the identification, acquisition and analysis of digital evidence originating from much more than just computers, such as smartphones, tablets, Internet of Things Devices, or data stored in the cloud[ii].

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations[iii]. 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 places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud.

The process of examining, interpreting, or reconstructing digital evidence on computers, networks, or the web is referred to as digital forensics. It's more than just finding evidence, however, a digital forensic specialist also has to be aware of the law to ensure that what they find is accepted by a court, no matter what kind of investigation is ongoing. The evidence gathered from digital forensics can be helpful in authenticating the source of a document or some software, or even to catch a criminal committing cybercrime. This is why digital forensic specialists may be used in law enforcement[iv], open investigations, and even in cyber security.

Just as physical crime scenes are kept as undisturbed as possible, its best when digital crime scenes are untouched so that the data obtained is pure and uninfluenced. When you open a program or a document, you leave a trace, even if you do not save it. When a system is procured that is suspected to be related to a case, it's usually required that no one touch or make changes to the system until a digital forensics investigator gets a chance to obtain any evidence that can be found on the system. This is particularly true in cases where you have to establish that there were particular files were accessed, the methods used to access them, and the timeline of events.

In the process of collecting digital evidence, an investigator usually starts by getting a precise clone of the system at the time it was copied. Oftentimes, a device called a write-blocker is used, which allows copies to be made of a system that is shut down. There are cases where investigators are unable to shut down a system for fear that some evidence may disappear. In such a situation, specialists would use a "live acquisition" technique that runs a diagnostic program on the system in question, copying information into the specialist's drive. Investigators have to be sure that they have due cause to obtain data from a system, otherwise evidence obtained throughout the investigation could be deemed inadmissible.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Civil cases on the other hand deal with protecting the rights and property of individuals (often associated with family disputes) but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (eDiscovery) may be involved.

Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion). This standard provides guidance on identifying, gathering/collecting/acquiring, handling and protecting/preserving digital forensic evidence that is, "digital data that may be of evidential value" for use in court.

The fundamental purpose of the ISO27k digital forensics[v]standards is to promote good practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardisation will (eventually) lead to the adoption of similar if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

One of the most critical issues in forensic investigations is the acquisition and preservation of evidence in such a way as to ensure its integrity. As with conventional physical evidence, it is crucial for the first and subsequent responders (defined as "Digital Evidence First Responders" and "Digital Evidence Specialists") to maintain the chain of custody of all digital forensic evidence, ensuring that it is gathered and protected through structured processes that are

acceptable to the courts. More than simply providing integrity, the processes must provide assurance that nothing untoward can have occurred. This requires that a defined baseline level of information security controls is met or exceeded.

Digital forensic evidence can come from any electronic storage or communications media such as cell phones, computers, iPod's and video game consoles[vi]. By its nature, digital forensic evidence is fragile it can be easily damaged or altered due to improper handling, whether by accident or on purpose.

Prior to the release of ISO/IEC 27037, there were no globally-accepted standards on acquiring digital evidence, the first step in the process. Police have developed their own national guidelines and procedures for the acquisition and protection of electronic evidence. However, this creates issues when cross-border crimes are committed since digital forensic evidence acquired in one country may need to be presented in the courts of another. Tainted evidence that may have been acquired or protected without the requisite level of security may be legally inadmissible[vii].

This article aims to identify success factors and challenges in digital forensic for law enforcement based on available scientific literature and findings.

DATA SOURCES USED IN A FORENSICS INVESTIGATION

Forensic analysis requires the acquisition and management of many different types of evidence, including individual disk drives, RAID sets, network packets, memory images, and extracted files[viii]. In recent years understanding these sources along with their relevance in different types of investigations has become paramount in the field of digital forensics. The sections that follow cover four main data sources are used in digital forensics. These sources include system logs, file systems, intrusion detection and prevention systems, and computer memory images

System logs

Syslog and RSyslog, are log files that contain entries (or messages) from different application services such as an apache web server. They also provide hooks into web applications and other services that can provide additional insight into for example an enterprise Content Management

System, or an online inventory management system. SysLog is typically used in Linux or Unix based environments. It captures events not only from the operating system and hosted applications, but also other servers connected to the infrastructure such as database systems. It is typically used by systems administrators and software developers to keep an eye on the overall health of systems. In addition to monitoring for general messages, errors, and events triggered by applications, it also provides a good data source for forensics examination.

File systems

Hackers are increasingly using a technique, known as steganography, to trick internet users and smuggle malicious payloads past security scanners and firewalls. Newman (2017)[ix]. The term 'Steganography' refers to 'covered writing' and encompasses methods of transmitting secret messages through innocuous cover carriers in a manner that their existence is undetectable[x]. Malicious code or malware often uses covert means to hide within a file systems application code. Operating System (OS) file systems are often used by attackers to their advantage in embedding such code within a sever.

Intrusion detection and prevention systems

Earlier in this paper, logs were discussed in terms of their relevance to various security incidents. Another means to providing more transparency into a system where various incidents may have happened is through the use of an Intrusion Detection System (IDS). Intrusion Detection Systems (IDS) come in various forms and provide different functionality. Host based systems are by their very name concerned with the host it is attached to. When the first intrusion-detection tools were designed, the target environment was a mainframe computer, and all users were local to the system considered[xi]. Host based IDS therefore evolved from this mentality to their current form which are typically software based and reside on a single host or computer. Network based IDS on the other hand are used to capture and analyse packets of data sent across an entire network. Another term called Intrusion Prevention Systems (IPS) is an IDS that also performs actions based on a set of criteria that alert the system based on suspicious traffic. The terms IDS and IPS are often interchangeable, however in a forensics investigation, the aftermath of an incident is usually what is of concern and any data captured will help support analysis.

Memory images

During a digital forensics investigation, those carrying out the analysis on various data sources may have a limited time to capture important data from volatile sources such as memory. A memory image is essentially a snapshot of all information captured in a systems Random Access Memory (RAM) that is by its very nature volatile. In a typical computer system, as soon as it is shut down, contents within memory are destroyed. In addition to this, memory is not in a static state and is forever changing depending on user interactions, services and other application calls within the system. It is therefore essential that a forensics expert can recover a memory image as quickly as possible before any important evidence is modified or destroyed[xii].

FORENSIC DIGITAL EVIDENCE

Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence. For example, mobile devices use online-based based backup systems, also known as the "cloud", that provide forensic investigators with access to text messages and pictures taken from a particular phone. These systems keep an average of 1,000-1,500 or more of the last text messages sent to and received from that phone.

In addition, many mobile devices store information about the locations where the device travelled and when it was there. To gain this knowledge, investigators can access an average of the last 200 cell locations accessed by a mobile device. Satellite navigation systems and satellite radios in cars can provide similar information. Even photos posted to social media such as Facebook may contain location information. Photos taken with a Global Positioning System (GPS) enabled device contain file data that shows when and exactly where a photo was taken. By gaining a subpoena for a particular mobile device account, investigators can collect a great deal of history related to a device and the person using it.

Who Conducts the Analysis

According to the National Institute of Justice[xiii], "Digital evidence should be examined only by those trained specifically for that purpose." With the wide variety of electronic devices in use today and the speed with which they change, keeping up can be very difficult for local law

enforcement. Many agencies do not have a digital evidence expert on hand[xiv] and, if they do, the officer might be a specialist in cell phones but not social media or bank fraud. A detective may be able to log onto e-Bay® and look for stolen property but may be unable to capture cell phone text message histories and could destroy evidence just by trying. Many take an interest in the area and learn what they can, but there is no single path to digital evidence expertise qualifications and certifications are not standardized across the country. Incorporation of digital seizure techniques is becoming more widespread in first responder training.

Certified Digital Media Examiners are investigators who have the education, training and experience to properly exploit this sensitive evidence. That said, there is no single certifying body, and certification programs can contain different courses of study. Generally speaking, these professionals have demonstrated core competencies in pre-examination procedures and legal issues, media assessment and analysis, data recovery, specific analysis of recovered data, documentation and reporting, and presentation of findings. While certification of examiners is not required in most agencies, it is becoming a widely valued asset and the numbers of certified examiners will increase. Vendor-neutral (not software based, but theory- and process-based) certification is offered through the Digital Forensics Certification Board (DFCB), an independent certifying organization for digital evidence examiners, the National Computer Forensics Academy at the High Tech Crime Institute and some colleges.

Most states have at least one laboratory or section for digital forensics and a variety of task forces including Internet Crimes against Children (ICAC), Joint Terrorism Task Force (JTTF), and Narcotics and Property Crimes. These forces comprise officers with specialized training, including search, seizure and exploitation of digital evidence as it pertains to their area of expertise. Agencies and investigators must work together to ensure the highest level of security and evidence handling is used. In the United States, the FBI can provide assistance in some specialty areas.

In Cameroon[xv], we have laws[xvi] and organs like Law N° 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality (hereinafter referred to as Cyber law)[xvii], National Agency for Information and Communication Technologies (ANTIC), UNGA Resolution: Creation of a Global Culture of Cyber Security and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211, Law No. 2016/007 of 12 July 2016

relating to the Penal Code, Regulation No. 01/CEMAC/UMAC/CM of 4th April 2003 on the Prevention and Suppression of Money Laundering and Financing Terrorism in Central Africa.

A range of public institutions provide the foundation for development of ICT in government which are directly or indirect linked to digital forensics challenges in general and cyber criminality in particular[xviii]. The Telecommunications Regulatory Board[xix] (TRB) under the auspices of MINPOSTEL, the computer divisions in government departments and the National Centre for the Development of Computer Services (CENADI) are the relevant organisations and are all available online. Furthermore, major e-government initiatives were taken in relation to the computerisation of records, including state personnel and salaries (SIGIPES), public finances (SIGEFI), customs transactions (SYDONIA), transport titles (driving licence, car ownership) (SYSTAC) and electoral documents (ELECAM). The PRIMO project provides online tender documents[xx]. Each of these e-administration programmes requires network security and ways of preventing or reducing cybercrime[xxi].

Equally important are initiatives in ICT infrastructure development, including establishment of RASCOM, to provide access to satellite resources and investment in access to the SAT3 undersea cable system for access to international bandwidth. There is ongoing deployment of approximately 3 200km of fibre optic cable nationwide, in partnership with Huawei.

The emerging reality is that the country's public administration is in transition to e-processes. If digital government is dawning for Cameroon's population of approximately 18 million people, then online security is important for resilience, continuity, sustainability and further development[xxii]. Some decided cases could be illustrative in the fight against cybercrimes in Cameroon.

The case of ***The People of Cameroon v Ekume Otte Sakwe***[xxiii] is illustrative of this point. In casu, Sakwe, a resident in Buea was charged by the judicial police officer for publication of force information about three companies which were Yadikwa Immobilier, Agro Agricultural Cooperative Ltd and Darling Home without being able to attest its veracity thereby committing an offence punishable by section 78 (1) of the Law. After examination by the examining magistrate, Sakwe walked away a free man for want of concrete evidence.

Similarly, in ***The People of Cameroon v Tamukum Fonjiyang Ferdinand and Song Charles Waindim*** [xxiv], the accused were examined by the examining magistrate for publication of false information that they had puppies to sell when in fact did not have. After full hearing and consideration of evidence tendered before the court of First Instance of Buea, the accused were found not guilty on the count of cybercrime (pet scam) and so were consequently acquitted. Also, the Law punishes anyone who for financial gain, uses any means to introduces, alter, erase or delete electronic data such as to cause damage to someone else's property[xxv]. This was the situation in ***The People of Cameroon v Kadji Valery***[xxvi]. In this case, Kadji, a student of the University of Buea, fraudulently acquired a sum of money from a lady in Yaoundé. The matter was reported to ANTIC which investigated into the matter and traced Kadji"s account at BICEC Buea which was credited with the sum of 1,090,000 CFA francs. With this, ANTIC held that Kadji could not have had such an amount in his account if not of scamming and so was charged under section 73 (2) of the Law[xxvii]. Unfortunately, the case was discharged for lack of evidence to show that the money in his account was gotten from illegal act. This is one of the complications of proving scamming and other cybercrimes in the country.

How Digital Devices are Collected

- **On the scene**[xxviii]

As anyone who has dropped a cell phone in a lake or had their computer damaged in a move or a thunderstorm knows, digitally stored information is very sensitive and easily lost. There are general best practices, developed by organisations like SWGDE and NIJ, to properly seize devices and computers. Once the scene has been secured and legal authority to seize the evidence has been confirmed, devices can be collected. Any passwords, codes or PINs should be gathered from the individuals involved, if possible, and associated chargers, cables, peripherals, and manuals should be collected. Thumb drives, cell phones, hard drives and the like are examined using different tools and techniques, and this is most often done in a specialized laboratory.

First responders need to take special care with digital devices in addition to normal evidence collection procedures to prevent exposure to things like extreme temperatures, static electricity and moisture.

- **Seizing[xxix]Mobile Devices**

Devices should be turned off immediately and batteries removed, if possible. Turning off the phone preserves cell tower location information and call logs, and prevents the phone from being used, which could change the data on the phone. In addition, if the device remains on, remote destruction commands could be used without the investigator's knowledge. Some phones have an automatic timer to turn on the phone for updates, which could compromise data, so battery removal is optimal.

If the device cannot be turned off, then it must be isolated from its cell tower by placing it in a Faraday bag or other blocking material, set to airplane mode, or the Wi-Fi, Bluetooth or other communications system must be disabled. Digital devices should be placed in antistatic packaging such as paper bags or envelopes and cardboard boxes. Plastic should be avoided as it can convey static electricity or allow a build-up of condensation or humidity. In emergency or life threatening situations, information from the phone can be removed and saved at the scene, but great care must be taken in the documentation of the action and the preservation of the data.

When sending digital devices to the laboratory, the investigator must indicate the type of information being sought, for instance phone numbers and call histories from a cell phone, emails, documents and messages from a computer, or images on a tablet.

- **Seizing Stand Alone Computers and Equipment**

To prevent the alteration of digital evidence during collection, first responders should first document any activity on the computer, components, or devices by taking a photograph and recording any information on the screen. Responders may move a mouse (without pressing buttons or moving the wheel) to determine if something is on the screen. If the computer is on, calling on a computer forensic expert is highly recommended as connections to criminal activity may be lost by turning off the computer. If a computer is on but is running destructive software (formatting, deleting, removing or wiping information), power to the computer should be disconnected immediately to preserve whatever is left on the machine[xxx].

Office environments provide a challenging collection situation due to networking, potential loss of evidence and liabilities to the agency outside of the criminal investigation. For instance,

if a server is turned off during seizure that is providing a service to outside customers, the loss of service to the customer may be very damaging. In addition, office equipment that could contain evidence such as copiers, scanners, security cameras, facsimile machines, pagers and caller ID units should be collected.

Computers that are off may be collected into evidence as per usual agency digital evidence procedures.

How and Where the Analysis is Performed

Once the digital evidence has been sent to the laboratory, a qualified analyst will take the following steps to retrieve and analyse data:

- **Prevent contamination:**

It is easy to understand cross contamination in a DNA laboratory or at the crime scene, but digital evidence has similar issues which must be prevented by the collection officer. Prior to analysing digital evidence, an image or work copy of the original storage device is created. When collecting data from a suspect device, the copy must be stored on another form of media to keep the original pristine. Analysts must use "clean" storage media to prevent contamination or the introduction of data from another source. For example, if the analyst was to put a copy of the suspect device on a CD that already contained information, that information might be analysed as though it had been on the suspect device. Although digital storage media such as thumb drives and data cards are reusable, simply erasing the data and replacing it with new evidence is not sufficient. The destination storage unit must be new or, if reused, it must be forensically "wiped" prior to use. This removes all content, known and unknown, from the media.

- **Isolate Wireless Devices:**

Cell phones and other wireless devices should be initially examined in an isolation chamber, if available. This prevents connection to any networks and keeps evidence as pristine as possible. The Faraday bag can be opened inside the chamber and the device can be exploited, including phone information, Federal Communications Commission (FCC) information, SIM cards, etc. The device can be connected to analysis software from within the chamber. If an agency does

not have an isolation chamber, investigators will typically place the device in a Faraday bag and switch the phone to airplane mode to prevent reception.

- **Install write-blocking software:**

  To prevent any change to the data on the device or media, the analyst will install a block on the working copy so that data may be viewed but nothing can be changed or added.

- **Select extraction methods:**

  Once the working copy is created, the analyst will determine the make and model of the device and select extraction software designed to most completely "parse the data," or view its contents.

- **Submit device or original media for traditional evidence examination:**

  When the data has been removed, the device is sent back into evidence. There may be DNA, trace, fingerprint, or other evidence that may be obtained from it and the digital analyst can now work without it. Learn more about DNA, trace evidence, or fingerprints,

- **Proceed with investigation:**

  At this point, the analyst will use the selected software to view data. The analyst will be able to see all the files on the drive, can see if areas are hidden and may even be able to restore organization of files allowing hidden areas to be viewed. Deleted files are also visible, as long as they haven't been over-written by new data. Partially deleted files can be of value as well.

Files on a computer or other device are not the only evidence that can be gathered. The analyst may have to work beyond the hardware to find evidence that resides on the Internet including chat rooms, instant messaging, websites and other networks of participants or information. By using the system of Internet addresses, email header information, time stamps on messaging and other encrypted data, the analyst can piece together strings of interactions that provide a picture of activity[xxxi].

DIGITAL EVIDENCE AND TRADITIONAL EVIDENCE: OBTAINING LEGALITY OF THE PROCESS

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 places. Digital evidence is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud.

The collection and preservation of digital evidence differs in many ways from the methods law enforcement officers are used to using for traditional types of evidence. Digital evidence is intangible, a magnetic or electronic representation of information. Its physical form does not readily reveal its nature.

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.[xxxii]As concerns Cameroon, Part III of the 2010 LAW N° 2010/012 OF 21 December 2010, law relating to cyber security and cyber criminality 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[xxxiii].

THE WAYS IN WHICH DIGITAL EVIDENCE IS AUTHENTICATED AND RELIABLE

The process of determining whether evidence is worthy is called authentication. Authentication is actually a two-step process, with an initial examination of the evidence to determine that it is what its proponent claims and, later, a closer analysis to determine its probative value.

The process of determining whether evidence is worthy is called authentication. Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is

accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record.[xxxiv]

Authentication is actually a two-step process, with an initial examination of the evidence to determine that it is what its proponent claims and, later, a closer analysis to determine its probative value. In the initial stage, it may be sufficient for an individual who is familiar with the digital evidence to testify to its authenticity. For instance, the individual who collected the evidence can confirm that the evidence presented in court is the same as when it was collected. Alternately, a system administrator can testify that log files presented in court originated from her/his system.

In some cases, the defences will cast doubt on more malleable forms of digital evidence, such as logs of online chat sessions.

In the of ***Michigan v. Miller 2002***[xxxv], in 2000, e-mail and AOL Instant Messages provided the compelling evidence to convict Sharee Miller of conspiring to kill her husband and abetting the suicide of the admitted killer[xxxvi] she had seduced with the assistance of the Internet. Miller carefully controlled the killer's perception of her husband, going so far as to masquerade as her husband to send the killer offensive messages. In this case, the authenticity of the AOL Instant Messages was questioned in light of the possibility that such an online conversation could be staged[xxxvii].

In ***United States v. Tank***[xxxviii], a case related to the Orchid/Wonderland Club investigation, the defendant argued that the authenticity and relevance of Internet chat logs was not adequately established. One of the points the defence argued was that the chat logs could be easily modified. The prosecution used a number of witnesses to establish that the logs were authentic. The court held that "printouts of computer-generated logs of 'chat room' discussions may be established by evidence showing how they were prepared, their accuracy in representing the conversations, and their connection to the defendant." This case is significant because it is one of the first to deal with the authentication of chat logs. However, some feel that there are still questions about the authenticity and reliability of Internet chat logs that have not been addressed. On IRC, for example, in addition to the chat channel window, there may be important information in other areas of an IRC client such as the status window and in private

chat or fserve windows. Since it is not possible for one investigator simultaneously to view every window, we must rely heavily on the logs for an account of what occurred. In some instances, investigators have been able to compensate for a lack of documentation by testifying that the evidence being presented is authentic and reliable. Of course, it is best to have solid documentation.

To authenticate digital evidence, it may also be necessary to demonstrate that a computer system or process that generated digital evidence was working properly during the relevant time period. For instance, the section in the Federal Rules of Evidence 901(b)(9) titled "Requirement of Authentication or Identification" includes "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." In the United Kingdom, under Section 69 of the PACE, there is a formal requirement for a positive assertion that the computer systems involved were working properly.

EVALUATION DIGITAL FORENSICS PROCESS MODELS

With increased use of technology in organizations and rapid changes in technology cyber forensic process is also advancing into new ways. In this context, organizations also need to align their technological infrastructure to meet the challenges in conducting successful process of forensic investigations to attain maximum and desired benefits of it

The first digital forensic process model proposed contains four steps: Acquisition, Identification, Evaluation and Admission.[xxxix]. These models attempt to speed up the entire investigative process or solve several of problems commonly encountered in the forensic investigation. Since then, numerous process models have been proposed to explain the steps of identifying, acquiring, analysing, storage, and reporting on the evidence obtained from various digital devices. In recent years, an increasing number of more sophisticated process models have been proposed. These models attempt to speed up the entire investigative process or solve several of problems commonly encountered in the forensic investigation. In the last decade, cloud computing has emerged as a disruptive technological concept, and most leading enterprises such as IBM, Amazon, Google, and Microsoft have set up their own cloud-based services. In the field of digital forensic investigation, moving to a cloud-based evidence processing model would be extremely beneficial and preliminary attempts have been made in

its implementation. Moving towards a Digital Forensics as a Service model would not only expedite the investigative process, but can also result in significant cost savings – freeing up digital forensic experts and law enforcement personnel to progress their caseload.

Process Models

Even though digital forensics is a relatively new research area, it has already made significant progress. The progress is not only from a technology perspective, such as tools to collect and analysis digital evidence, but also with the improvement of methodology. In digital forensics, a process model is the methodology used to conduct an investigation; a framework with a number of phases to guide an investigation. Generally, process models were proposed on the experience of previous work. Due to the variety of cases, for example, cyber-attacks conducted by IT specialists, civil cases in a corporation, or criminal cases, different investigators tend to follow different methods in their investigative process, there is no standard workflow in digital forensic investigation.

A standard methodology in digital forensics investigation consists of a definition of the sequence of actions necessary in the investigation. A framework, if it is too simplistic or has fewer phases, might not provide much guidance to the investigation process. A framework with more phases and each phase with sub-steps, with more limitation of its usage scenario may prove more useful. Even though it is almost impossible to design a perfect process model that can deal with any investigation, an ideal framework should be general, which means that it could be applied to as many cases as possible. Furthermore, considering that techniques evolve so fast, a well-defined framework should also with the capability to adopt new techniques in the process of investigation.

Numerous process models have been proposed in the literature to date. Generally, each framework attempts to refine the standard methodology for a specific use case and each of these process models take a broadly similar approach. The earliest research concentrated on defining the process of digital forensic investigation[xl]. More recently, process model research centres around solving more specific issues specific use cases or focus on particular steps (evidence collection, preservation or examination, analysis). The triage model[xli]is effective for cases that are time sensitive. By employing digital forensics triage, investigators could discover

pertinent evidence and the police could get leads about the criminal sooner instead having to wait for the whole report which could take several months or even years.

The Evolution of Digital Forensic Process Models

Several process models have been proposed to date. Current models can be categorised into three main types:

- The first type consists of general models that define the entire process of digital forensic investigation. These models were proposed from 2000 to 2010. Through that time, precisely what should be done and the order to do each step in a digital forensic investigation was still somewhat controversial.

- The second type focus on a particular step in the investigation process or a specific kind of investigative case;

- The third type defined new problems and/or explored new methods or tools to address specific issues.

Early Digital Forensic Process Models

At the turn of the century, it was still the early days of research on digital forensics and digital forensic process models. Initially, one of the most urgent issues in digital forensics was to define a process model to make the entire investigative process consistent and standardised. A number of general digital forensic processing models have been defined. Most of these frameworks define a group of necessary steps in a whole investigation process, and the models were refined over time. The later models improve upon the former ones by including some additional steps or defining sub-steps of the process models making each step more precisely defined.

The traditional framework had been refined and formed a number of novel frameworks. Some inheritance relation among the existing frameworks listed below:

- DFRWS model [xlii] => SRDFIM[xliii]

- DFRWS model[xliv] => An Abstract Digital Forensics Model[xlv]

- IDIP[xlvi] & DCSA[xlvii] => CFFTPM[xlviii]

- Integrated Digital Investigation Process (IDIP)[xlix] => Enhanced Integrated Digital Investigation Process (EIDIP)[l].

- Integrated Digital Forensic Process Model[li] => DFaaS Process Model[lii]

The focus of these models is to define the phases on typical investigations, the sequence of these phases and the definition of the key concepts of each phase[liii].

Henry Lee proposed a Scientific Crime Scene Investigation (SCSI) model for digital forensic investigation in 2001[liv]. Ciardhuáin[lv]criticises the SCSI model is not a systematic digital forensic process model as it only focuses on physical crime scene investigation and lack of describing on digital criminal scene investigation. Kohn[lvi] explained that the physical crime scene investigation process can be adapted to digital crime scene investigation. The Event-based Digital Forensic Investigation Framework separates the concepts of the physical crime scene and the digital crime scene, collecting digital devices from the physical crime scene and then obtaining digital evidence from the digital devices' storage[lvii]. In 2000, Casey defined a digital forensic process model and was refined further in 2004. Casey's model focuses on digital evidence processing and examining. The Enhanced Integrated Digital Investigation Process (EIDIP) model was proposed by Baryamureeba and Tushabe[lviii]. The EIDIP model is based on IDIP, and introduces a trace back phase to address the problem of having to reconstructing twice in IDIP.

Refining Digital Forensic Process Models

Merely following a general process model is often not specific enough to handle the broad range of cases typically encountered by law enforcement. The criminal could be an IT specialist and conduct advanced cybercrimes, CCTV cameras' storage may need to be analysed, or data leakage in a corporation, etc. These different situations often require bespoke methodologies.

After the general process procedure was clearly defined, researchers started working on specific issues that are more detailed. For example: 1) refining a process model by make an improvement at a specific step of the investigation; 2) dealing only with a specific category of cases, such as, network forensics and mobile devices forensics; 3) Triage models[lix]outline

specific processes for time sensitive cases, such as child abductions, missing person cases and so on.

Extended Model of Cybercrime Investigation

In 2004, several process models had already been defined. However, each did not include a significant aspect of cybercrime investigation itself. An extended model of cybercrime investigation was proposed by Ciardhuáin[lx]. This model follows a waterfall fashion and the necessary activities are conducted in sequence. This model allows iteration in some part of the investigation, for example, the iterative process of "examination - hypothesis - presentation - proof/defence".

Digital Forensic Triage Process Model

In some special cases, such as kidnaps and hostage rescue, acquiring clues from digital devices immediately is crucial, or some other cases such as robbery, crucial information is required as soon as possible to increase the likelihood of catching the criminal before they have escaped to another country. Often traditional models are insufficient for this use case - potentially taking weeks or years to get results. Tiered models are designed to expedite situations like this. Considering traditional models are designed to guide the entire investigation, a triage process model was proposed to deal with time sensitive cases[lxi]. This model focuses on the crucial first few hours of an investigation.

Digital Forensic Model Based on Malaysian Investigation Process

This model is notable in that it is focused on data acquisition process, including more detailed handling on live data acquisition and static data acquisition in cybercrime investigation[lxii].

The Systematic Digital Forensics Investigation Model

This model is focus on computer fraud and cybercrimes, which is helpful in evidence dynamics and reconstruction[lxiii].

Integrated Digital Forensic Process Model

This model is the most recent proposed process model which including a relative generally digital forensic investigation[lxiv].

Recent Research on Digital Forensic Process Models

Some new and popular technologies result in new problems hindering digital forensics investigations. Cloud computing makes evidence collection more difficult; Internet-of-Things adds a variety of new device and storage forms; more digital devices connected into the Internet result in an ever-increasing volume of data. In recent years, research on process models is more focused on integrating other technologies, such as data mining, to support the original models, or propose novel process models to solve the issues caused by these new technologies.

Some recent models, include:

- An integrated conceptual digital forensic framework for cloud computing[lxv].
- Data reduction and data mining framework[lxvi].
- Internet of Things (IoT) Based Digital Forensic Model[lxvii].

An Integrated Conceptual Digital Forensic Framework for Cloud Computing

As the prevalence of cloud computing services increases, collecting digital evidence from a remote server, which often is stored in another jurisdiction, has become necessary. In recent years, researchers in digital forensics have been trying to address the issues encountered in Cloud Forensics. An integrated conceptual digital forensic framework was proposed by Martini and Choo[lxviii]based on two widely used basic models[lxix]. The difficulties encountered conducting a forensic investigation of a cloud service can be identified in each stage of a typical case. Firstly, the determination that cloud forensics is necessary might only be possible after acquiring cached information or stored login credentials from a physical digital device, such as a laptop or smartphone. It is as if the investigator opens one door (physical digital evidence devices) and gets a key of the other (cloud evidence). If the first key was not discovered (or example, lost through mishandling of volatile data), there is no possibility to get the second key. As the result, the investigator would never retrieve any evidence behind the second door. Secondly, in the collection of cloud evidence, the problems often found include: 1) no possibility to physically seizing all the servers in a cloud computing environment; 2) the server could be in another jurisdiction; 3) the collection of metadata might not be possible just to name a few.

Data Reduction and Data Mining Framework

Considering the new challenges encountered in digital forensic investigation, Quick and Choo[lxx]list seven requirements of forensic analysis: faster collection, reduced storage, timely review, intelligence, research, knowledge management, archive and retrieval. One challenge in digital forensics is the ever-increasing volume of data, which has impeded investigations from a number of standpoints including evidence collection, data preservation and analysis. The growth of digital evidence has been ongoing for many years and is safely predicted to increase further into the future. The core idea of this framework is to acquire a subset of the data by utilising data reduction and conduct intelligence analysis through data mining. Obviously, the subset prioritises files which are the most crucial and important for investigation. This subset is much smaller than the entirety of the evidential data, and as a result, any operations investigators conduct on it would be significantly faster. This subset of data could bring number of significant benefits for investigation:

- Triage devices and media;

- Faster indexing;

- Provide potential to utilise data mining or intelligence analysis;

- Cross-case analysis;

- Enable research of historical case data and intelligence analysis.

Internet of Things Based Digital Forensic Model

The growing prevalence of Internet-of-Things (IoT) brings with it new problems for digital forensics. As a new challenge in this area, the volume of digital devices needing to be collected, analysed, examined and preserved, as well as the variety of storage formats make analysis more arduous. A more sophisticated forensic model, which aims to address the specific issues relating to IoT based investigation, is that proposed by Perumal[lxxi]. This model defines a standard operating procedure for investigation of IoT devices.

Field Processing Model

One of the more recent models proposed surrounds a digital forensic field processing model[lxxii]. This model is focused on training non-digital evidence to specialists conducting the early stage of investigation on scene. The front-line investigators analyse the pertinent information first and a more detailed examination and analysis will be subsequently conducted in the laboratory. This research on one hand solves the problem of the shortage of digital forensic specialists in law enforcement, and on the other hand helps relieve the digital forensic backlog. Coupling DFaaS with this field triage processing model could result in significant benefits. Namely, the traditional laboratory-based examination could be conducted on scene through a laptop connected with the cloud system. This would afford the investigator the use of a powerful computing resource in the field.

POLICIES AND PROCEDURES OF HANDLING CYBER FORENSIC EVIDENCE

As society embraces technology and the use of mobile devices increases, a growing number of technological devices are being used in crimes and then seized by law enforcement as evidence. These devices are used by criminals to communicate, store data, and facilitate crimes. Computers, cell phones, GPS devices, digital cameras, and other devices that contain digital evidence must be properly collected, handled, and processed. The volatile nature of the data on these devices requires proper seizure to preserve the integrity of the data and ensure their evidentiary value in legal proceedings. Devices must also be processed properly, whether the data they contain are incriminating or exculpatory. It is equally important that these devices are stored in a manner that will preserve the data in their original state for examination by the plaintiff or defences and for the introduction of the original item into court when necessary. Proper documentation for each device tracking it from initial submission through storage, processing, the release of any information related to the data on the device, and the return of the device back to the originating individual or entity will ensure the admissibility of the item and the resulting data in any judicial proceeding.

Case assignment and prioritisation

Cases involving digital evidence are received, prioritized, and assigned for forensic analysis. A system must be established to assign cases to lab personnel. Criteria for assignment include priority, case circumstances, examiner skill set, and forensic discipline.

This policy will establish the criteria for case assignment and prioritization and the authority to make an exception in case assignment or priority. Policy *CASE ASSIGNMENT* The forensic director or designee will assign all incoming cases. It is possible that a case may be assigned by forensic discipline based on the expertise or current caseload of the examiners or on the needs of the case itself.

Unless the submitting agency indicates a need for expedited processing, all cases will be assigned in the order received. *CASE PRIORITISATION* The forensic director or designee will be responsible for identifying cases with a higher priority than others. Priority level will be determined based on the facts known about each case when it is submitted to the digital forensic lab and will be updated as relevant information affecting the priority becomes available. In collaboration with the investigator, submitting agency, and prosecuting attorney, the forensic director will be responsible for identifying cases that may be eligible for early case assessment (ECA). ECA may enable the digital forensic examiners to perform a forensic examination of the submitted digital evidence only to the extent authorized by the legal proceedings and authorities. Additionally, cases may be triaged for specific information of investigative value to a case, such as contraband images in a child exploitation case. ECA and triage provide the forensic director and staff a way of improving the efficiency of justice and enable examiners to devote more time to more complex cases and cases that contain large volumes of digital evidence.

An example of case prioritisation

(1) Terrorism or any case where the loss of life is imminent.

(2) Violent crimes such as murder, rape, and assault

(3) A child at immediate risk of exploitation or abuse

(4) Child pornography and solicitation

(5) Theft or destruction of intellectual property and public corruption

(6) Financial crimes

(7) Internet crimes, including network intrusion and unauthorized access

(8) Identity theft

Equipment testing, validation, and updates

All equipment and software used by digital forensic personnel must first be tested and validated to confirm that it is operating as designed and producing accurate, valid results. Testing and validation must be repeated each time the equipment, firmware, and software are upgraded, reinstalled, or modified. The results of all testing and validation will be recorded and kept on file in order to document that all equipment being used in the collection and processing of digital evidence is functioning within the manufacturer's specifications and the examiner's expectations based on training and experience.

Validation testing will be conducted by all examiners who use any of the collection and processing hardware or software, in any fashion or to any degree, to collect or process digital evidence in the digital forensic lab or at a crime scene.

Validation procedures

- No forensic equipment will be used in the digital forensic lab prior to being tested and validated by forensic personnel and approved by the forensic director.

- Examiners will test each item of hardware and software in a manner consistent with the manufacturer's specifications of usage. Testing will be performed using the same datasets for standardization. All results and anomalies will be documented.

- Digital Evidence Handling Policy Examiners performing the validation testing on all forensic hardware and software will use a standardized testing and report form, including the date of validation, product name, version number, manufacturer, and cost. All of the validation reports for each item of hardware and software will be approved by the forensic director before those items are used in the lab, and all the

reports will be maintained on the digital forensic lab server (if available) and also in paper format in a binder maintained within the lab.

- All hardware and software will be registered in the company's name. If the registration must be to an individual, approval from the forensic director will be obtained in a memo format, with a copy of the memo maintained on the lab server (if available) and in the lab validation report binder.

Maintaining validations

When a piece of equipment becomes damaged or is showing signs of wear or age, it should be tested to verify that it is still operating within the manufacturer's specifications. It is the responsibility of the examiners using the forensic equipment or assigned the item to report such issues to the forensic director. The forensic director will decide whether to replace faulty, damaged, or worn equipment.

Evidence and property handling

In order for devices that contain digital evidence to be properly introduced in any judicial proceeding, the devices must be tracked from the time they enter the custody of the lab through their release to the submitting entity. There must be a complete, documented chain of custody from intake to release of each device.

CONCLUSION AND WAY FORWARD

The rapid progress in technology has changed how people interact, communicate, work, and deal with data; and crime is not exempt from taking advantage of technological innovations. Criminals are early adopters of technology and have managed to integrate it into their illegal activities. Additionally, criminals have redesigned crime into cyber aided and cybercrimes. On the other hand, the diversity, quantity, and complexity of digital sources make it difficult for digital forensic practitioners to find digital evidence relevant to criminal investigations. Digital forensics is facing a wide variety of challenges, and researchers tend to focus their attention on challenges tackle by specific digital forensic disciplines like IoT forensics, cloud forensics, and multimedia forensics. Apart from the attention those disciplines deserve, a taxonomy of challenges in the field can facilitate addressing solutions where it is more required and suitable,

as well as orient future work aiming to improve the digital forensic domain. Some of these challenges[lxxiii]will be analyse subsequently in the form of recommendations.

- **Security[lxxiv]**

Security is a challenge in all e-government processes. With the growing number of personal data devices and other sophisticated technology, criminals are becoming better able to conceal their actions. Protecting critical network infrastructures requires a comprehensive view of security that combines physical, digital and procedural components. These components provide the level of cybersecurity necessary to guard against the many known and unknown threats in cyberspace. Cameroon's businesses, government administration and society depend to a high degree on the efficiency and security of ICT. Cybercrime can affect service providers, banks, petroleum data insurances, the stock exchange and the communication sector. Compromise on one network can allow an intruder either direct access to a partner's private data or indirect access by allowing a back door into the partner's network. Thus, cybersecurity law covers the ICT sector as a whole, not only the e-government component.

The virtualisation[lxxv] of services creates a number of challenges in respect of security and confidence. Specific threats to cybersecurity include use of unsecured networks; misconfiguration of computer systems; poor user and administrator education; poor software design; network and system design issues; substandard operational procedures and protocols; weak passwords; and lack of awareness or indifference[lxxvi].

- **Explosion of complexity**

Evidence is no longer confined within a single host but, rather, is scattered among different physical or virtual locations, such as online social networks, cloud resources, and personal network attached storage units. For this reason, more expertise, tools, and time are needed to completely and correctly reconstruct evidence. Partially automating some tasks has been highly criticized by the digital investigation community, because it could quickly deteriorate the quality of the investigation. The technological advances in and proliferation of novel services account for a dramatic increase in the complexity that forensics professionals must manage.

- **Development of standards**

Despite technological advances, files are still the most popular digital artifacts to be collected, categorized, and analysed. Thus, the research community has tried to agree on standard formats, schema, and ontologies but without much success. They add that investigations of cutting-edge cybercrimes might require processing information in a collaborative manner or using outsourced storage and computation. Therefore, a core step for the digital forensics community will be the development of proper standard formats and abstractions.

- **Privacy-preserving investigations**

Nowadays, people bring into cyberspace many aspects of their lives, primarily through online social networks or social media sites. Unfortunately, collecting information to reconstruct and locate an attack can severely violate users' privacy and is linked to other hurdles when cloud computing is involved.

- **Legitimacy**

Modern infrastructures are becoming complex and virtualized, often shifting their complexity at the border (such as in fog computing) or delegating some duties to third parties (such as in platform-as-a-service frameworks). Thus, say the authors, "an important challenge for modern digital forensics will be executing investigations legally, for instance, without violating laws in borderless scenarios.

- **Rise of anti-forensics techniques**

Defensive measures encompass encryption, obfuscation, and cloaking techniques, including information hiding. Cooperation among international jurisdictions notwithstanding, investigating cybercrime and collecting evidence is essential in building airtight cases for law enforcement. For that, security experts need the best tools to investigate.

Digital forensics is fundamental to investigations performed in a reality that's often tightly coupled with its cyber extension. Modern digital societies are subject to cybercriminal activities and fraud leading to economic losses or hazards for individuals. Therefore, the new wave of forensics tools should be engineered to support heterogeneous investigations, preserve privacy, and offer scalability.

- **Training initiatives**[lxxvii]

It is further necessary to introduce training initiatives to help combat cybercrime in order to deliver secure and effective e-government processes. Training should be conducted on a regular basis and private-public partnerships in training should form the basis for capacity building. In order to continue the development and delivery of effective cybercrime training to law enforcement officers at a regional level, it is necessary for them to partner with organisations and industry to create a network to take responsibility for the training programmes and offer appropriate academic qualifications. Academic institutions are in a position to use their considerable pool of research and education expertise to support both government and industry in the development of education programmes designed to facilitate the enhancement of skills and qualifications relevant to the area of cybercrime. This will help cut down the cost of implementing security measures.

The cyber law deals with key economic, legal and social issues that will enable Cameroon to take a quantum leap to effectiveness in its public service delivery. The 2010 e-laws, if appropriately implemented, can enhance effectiveness of e-applications. It is possible to conclude that these laws are vital for the enhancement, continuity and sustainability of digital government. Therefore the cybersecurity legal framework must be appropriately enforced for a secure, resilient, sustainable and continuous Cameroon network as critical infrastructures on which digital forensic depends.

- **Future Work**[lxxviii]

More work needs to be done in the identification of success factors and opportunities in the domain. An area that deserves more attention and investigation is human-related challenges. For instance, the psychological distress digital forensics can experience after continuous exposure to illicit content (like child sexual abuse) is a topic that has not captured enough attention from the researchers. This topic is particularly important because it can be addressed from different perspectives, which may require multi-disciplinary approaches.

REFERENCES

1- Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., (2011), "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security (IJCSS), 5(1).

2- André Boraine & Ngaundje Leno Doris, (2019), "The Fight against Cybercrime in Cameroon", International Journal of Computer (IJC) Volume 35.

3- Asongwe, P. (2010), "A model regulatory and legislative framework for Cameroon", Presentation to the 1st CTO Cybersecurity Conference, 16-18 June 2010, London.

4- Baryamureeba, V. and Tushabe, F., (2004), "The Enhanced Digital Investigation Process Model", In Proceedings of the Fourth Digital Forensic Research Workshop.

5- Bean, R. A., K.R. Bush, et al. (2003), "The impact of parental support, behavioural control, and psychological control on the academic achievement and self-esteem of African American and European American adolescents", Journal of Adolescent Research, 18(5).

6- Carnaghan, "An analysis of different data sources used in a forensics investigation",https://www.carnaghan.com/analysis-different-data-sources-used-forensics-investigation/, consulted on 30/09/2021 at 11:27 am

7- Carrier, B. and Spafford, E.H., (2003), "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, 2(2).

8- Carrier, B. and Spafford, E.H., (2004), "An Event-Based Digital Forensic Investigation Framework. In Digital Forensic Research Workshop.

9- Ciardhuáin, S.Ó., (2004), "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, 3(1).

10- Cohen, M., Garfinkel, S., & Schatz, B. (2009), "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow", Digital Investigation, 6.

11- Debar, H., Dacier, M., & Wespi, A. (1999), "Towards a taxonomy of intrusion-detection systems", Computer Networks 31.

12- Decree No. 98/197 of 8 September 1998 to lay down the organisation and functioning of the Telecommunications Regulatory Board

13- Decree No. 98/198 of 8 September 1998 to set up the Cameroon Telecommunications Corporation (CAMTEL);

14- Decree no.2011/1521 fixing the modalities for the application of law no.2010/021 of 21 December 2010 and article 7 of the UNCITRAL Model Law on Electronic Commerce.

15- Digital Evidence and Forensics, (2010). Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012)

16- Edie Diabe P., Lecture notes on ' Law of Information and Communication Technology' University of Douala, faculty of Law and Political Science, Department of English Law, 2021-2022 academic year (unpublished).

17- Electronic Crime Scene Investigation: A Guide for First Responders, 2nd ed, 2008. Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012)

18- Forensic Examination of Digital Evidence: A Guide for Law Enforcement, 2004. Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012)

19- Hitchcock, B., Le-Khac, N.-A and Scanlon, M., (2016), "Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists", Digital Investigation, 16.

20- Joan B.Ali, " Digital Forensics: Legality of the Process in Cameroon", International Journal of Computer (IJC) (2015) Volume 17, No 1.

21- Johnson, N. F., & Jajodia, S. (1998), "Steganalysis: The investigation of hidden information". In Information Technology Conference, IEEE.

22- Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., (2013), "Integrated Digital Forensic Process Model. Computers & Security", 38.

23- Law No. 2005/13 of 29 December 2005 to amend and supplement some provisions of Law No. 98/14 of 14 July 1998 to govern telecommunications in Cameroon.

24- Law No. 98/14 of 14 July 1998 to govern telecommunications in Cameroon;

25- Lee, H.C., Palmbach, T. and Miller, M.T., (2001), "Henry Lee's Crime Scene Handbook", Academic Press, pp. 1-10.

26- Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M., (2016), "Current Challenges and Future Research Areas for Digital Forensic Investigation", In Proceedings of 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL), Daytona Beach, Florida, USA.

27- Martini, B. and Choo, K.-K.R., (2012), "An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Digital Investigation", 9(2).

28- McKemmish, R., (1999), "What is Forensic Computing?", Australian Institute of Criminology Canberra.

29- Milagros. C., 'Success Factors and Challenges in Digital Forensics for Law Enforcement: A Systematic Literature Review' (LL.M. Thesis, University of Skovde 2021).

30- Mokube, P. (2010), "State of e-governance in Cameroon", Presentation at Seminar on Electronic Governance Cameroon, July 2010, Yaoundé.

31- Newman, L., H. (2017), "Hacker Lexicon: What is steganography? Wired. Retrieved from: https://www.wired.com/story/steganography-hacker-lexicon/

32- Palmer, G., (2001), "A Road Map for Digital Forensic Research". In First Digital Forensic Research Workshop, Utica, New York.

33- Perumal, S., Norwawi, N.M. and Raman, V., Internet of Things (IoT) Digital Forensic Investigation Model: TopDown Forensic Approach Methodology. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE.

34- Pollifroni, M. (2006), "Cybercrimes and egovernment applications: some empirical evidences", eGovernment Workshop '06 (eGOV06), 11 September 2006, Brunel University, West London.

35- Quick, D. and Choo, K.-K.R., (2014), "Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive". Trends and Issues in Crime and Criminal Justice 480(1).

36- Reith, M., Carr, C. and Gunsch, G., (2002), "An Examination of Digital Forensic Models". International Journal of Digital Evidence, 1(3).

37- Reith, M., Carr, C. and Gunsch, G., (2002), "An Examination of Digital Forensic Models". International Journal of Digital Evidence, 1(3).

38- Republic of Cameroon (2010a). Law No 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon, Republic of Cameroon, Yaoundé.

39- Republic of Cameroon (2010b). Law No 2010/013 of 21 December 2010 relating to electronic communications in Cameroon, Republic of Cameroon, Yaoundé.

40- Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S., (2006), "Computer Forensics Field Triage Process Model", In Proceedings of the conference on Digital Forensics, Security and Law (CDFSL 2006). Association of Digital Forensics, Security and Law.

41- Rogers, M., (2006), "DSCA: A Practical Approach to Digital Crime Scene Analysis", In Information Security Management Handbook, Fifth Edition, Volume 3.

42- U.S. Secret Service, Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders, Version 3, 2006. Public Intelligence.net. (accessed July 5, 2012)

43- Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon, " Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service", https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf, consulted on 02/10/2021 at 3pm.

ENDNOTES

[i] International cybercrime has now become so extensive, underground suppliers are cropping up on the dark web offering easy access to the tools, programming frameworks, and services required to carry out cyberattacks. A notable example is Tox, a ransomware construction kit discovered by McAfee Labs on the dark web in May 2015. Briefly, the Tox framework can be customized and used to spread and coordinate infections in return for 20 percent of every ransom paid.

[ii] See Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon, " Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service", https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf, consulted on 02/10/2021 at 3pm; p.1.

[iii]See https://www.google.com/search?q=DIGITAL+FORENSICS&oq=DIGITAL+FORENSICS&aqs=chrome..69i57.1028j0j15&sourceid=chrome&ie=UTF-8, consulted on 30/03/2023 at 9am.

[iv] Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M., 2016. Current Challenges and Future Research Areas for
Digital Forensic Investigation. In *Proceedings of 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, Daytona Beach, Florida, USA, pp. 9-20.

[v]See https://www.iso27001security.com/html/27037.html#:~:text=The%20fundamental%20purpose%20of%20the,and%20investigation%20of%20digital%20evidence, consulted on 31/03/2023 at 5:10pm

[vi] See https://nij.ojp.gov/digital-evidence-and-forensics, consulted on 31/03/2023 at 6pm

[vii]See Reith, M., Carr, C. and Gunsch, G., 2002. An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3), pp. 1–12.

[viii]See Cohen, M., Garfinkel, S., & Schatz, B. (2009). Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. Digital Investigation, 6, S57-S68.

[ix] See Newman, L., H. (2017). Hacker Lexicon: What is steganography? Wired. Retrieved from: https://www.wired.com/story/steganography-hacker-lexicon/

[x] See Johnson, N. F., & Jajodia, S. (1998, September). Steganalysis: The investigation of hidden information. In Information Technology Conference, 1998. IEEE (pp. 113-116). IEEE.

[xi] See Debar, H., Dacier, M., & Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. Computer Networks 31 (1999) 805-822.

[xii]See Ian Carnaghan, "An analysis of different data sources used in a forensics investigation",https://www.carnaghan.com/analysis-different-data-sources-used-forensics-investigation/, consulted on 30/09/2021 at 11:27 am

[xiii] See Digital Evidence and Forensics, 2010. Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012)

[xiv] 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.

[xv] Cameroon intends to use ICTs to build a people-centred, inclusive and development-oriented information society, where its citizens can create, access, utilise and share information and knowledge in a bid to achieve sustainable social and economic growth, which is one of the preconditions for poverty reduction and hence improvement of the quality of life of Cameroonians. Consequently, the President of the Republic, H.E. Paul Biya, strongly emphasised on November 30, 2002, that the effective emergence of an information society in Cameroon would help “strengthen unity between our peoples and combat inequalities by granting access to information and knowledge to most Cameroonians…” and, thus, “make the country better placed to enter the third millennium”. He has repeatedly invited Cameroonians of all works of life to adopt and use ICTs in their daily activities in an effort to combat poverty and exclusion from the information society. It is in this light that he set the tone in his November 3, 2004 speech, when he stated inter alia, “our country needs generalised Internet access”.

[xvi]See Republic of Cameroon (2010a). Law No 2010/012 of 21 December 2010 relating to cybersecurity and cyber criminality in Cameroon, Republic of Cameroon, Yaoundé. See also Republic of Cameroon (2010b). Law No 2010/013 of 21 December 2010 relating to electronic communications in Cameroon, Republic of Cameroon, Yaoundé.

[xvii] See André Boraine & Ngaundje Leno Doris, " The Fight against Cybercrime in Cameroon", International Journal of Computer (IJC) (2019) Volume 35, No 1, pp 87-100

[xviii] See Edie Diabe P., Lecture notes on ' Law Of Information And Communication Technology' University of Douala, faculty of Law and Political Science, Department of English Law, 2021-2022 academic year (unpublished) pp. 13-15.

[xix] The Telecommunications Regulatory Board (TRB) is the public institution particularly responsible for regulating, controlling and monitoring the activities of the telecommunications sector in Cameroon. It is placed under the supervisory authority of MINPOSTEL. It was set up by the 1998 law on telecommunications (see section 22(1) of that law). TRB's duties are spelled out in Section 22(2) and repeated in Article 3 (1) of Decree No. 98/197 of 8 September 1998 to lay down the organisation and functioning of the Telecommunications Regulatory Board as follows: "The Board… shall be responsible for regulating, controlling and monitoring the activities of businesses and operators involved in the telecommunications sector. It shall also ensure compliance with the principle of equality in the treatment of users in all telecommunications enterprises." Another important duty of the Board is to arbitrate in the event of disputes between operators of the sector concerning in particular « the interconnection or access to a telecommunications network, numbering, frequency disturbance and the sharing of infrastructure."

[xx]See Mokube, P. (2010). State of e-governance in Cameroon. Presentation at Seminar on Electronic Governance Cameroon, July 2010, Yaoundé.

[xxi]See Asongwe. P., 'e-Government and The Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges', The African Journal of Information and Communication Issue 12, 2012, pp.157-163.

[xxii] See Pollifroni, M. (2006). Cybercrimes and egovernment applications: some empirical evidences. eGovernment Workshop '06 (eGOV06), 11 September 2006, Brunel University, West London. See also Asongwe, P. (2010). A model regulatory and legislative framework for Cameroon. Presentation to the 1st CTO Cybersecurity Conference, 16-18 June 2010, London.

[xxiii] Court of First Instance of Buea (CFIB)/017b/2015 unreported

[xxiv]CFIB/015f/2012 unreported.

[xxv] Section 72, Cyber Law N° 2010/012 of 21 December 2010 relating to Cyber Security and Cyber Criminality

[xxvi] Court of First Instance of Buea/011A/2013 unreported.

[xxvii] Section 73 (2), Cyber Law provides „Whoever deliberately accepts to receive electronic communications payment using a forged or falsified payment, credit or cash withdrawal card shall be punished in accordance with Subsection 1 above".

[xxviii]See Electronic Crime Scene Investigation: A Guide for First Responders, 2nd ed, 2008. Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012)

[xxix]See U.S. Secret Service, Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders, Version 3, 2006. Public Intelligence.net. (accessed July 5, 2012)

[xxx] See Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, 2007. Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012) supra

[xxxi]See Forensic Examination of Digital Evidence: A Guide for Law Enforcement, 2004. Department of Justice, Office of Justice Programs, National Institute of Justice. (accessed July 5, 2012)

[xxxii] See Joan B.Ali, " Digital Forensics: Legality of the Process in Cameroon", International Journal of Computer (IJC) (2015) Volume 17, No 1, pp 35-44.

[xxxiii] Ibid

[xxxiv] See Hon. Paul W. Grimm et al., Authentication of Social Media Evidence, 36 AM. J. TRIAL ADVOC. 433, 459 (2013) ("A trial judge should admit the evidence if there is plausible evidence of authenticity produced by the proponent of the evidence and only speculation or conjecture not Facts by the opponent of the evidence about how, or by whom, it 'might' have been created.").

[xxxv] No. 98-10001 decided: January 04, 2000

[xxxvi]See https://abcnews.go.com/US/convicted-killer-sharee-miller-admits-planning-husbands-murder/story?id=82726866, consulted on 31/03/2023 at 11am.

[xxxvii] See Bean, R. A., K.R. Bush, et al. (2003). The impact of parental support, behavioural control, and psychological control on the academic achievement and self-esteem of African American and European American adolescents. Journal of Adolescent Research, 18(5), 523-541.

[xxxviii] No. 98-10001, U.S. Court of Appeals for the Ninth Circuit, Argued and Submitted October 4, 1999 and Decided January 4, 2000

[xxxix] See Xiaoyu Du, Nhien-An Le-Khac, and Mark Scanlon, " Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service", https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf, supra pp. 3-10.

[xl] See Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., 2013. Integrated Digital Forensic Process Model. Computers & Security, 38, pp. 103-115.

[xli] See Hitchcock, B., Le-Khac, N.-A and Scanlon, M., 2016. Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. Digital Investigation, 16, pp. S75–S85.see also Rogers, M., 2006. DSCA: A Practical Approach to Digital Crime Scene Analysis. In Information Security Management Handbook, Fifth Edition, Volume 3. pp. 601-614.

[xlii] See Palmer, G., 2001. A Road Map for Digital Forensic Research. In First Digital Forensic Research Workshop, Utica, New York. pp. 27-30.

[xliii] See Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., 2011. Systematic Digital Forensic Investigation Model. International Journal of Computer Science and Security (IJCSS), 5(1), pp. 118-131.

[xliv]See https://www.researchgate.net/figure/DFRWS-Investigative-ModelPalmer-2001_fig1_325959432, consulted on 31/03/2023 at 1pm

[xlv]See Reith, M., Carr, C. and Gunsch, G., 2002. An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3), pp. 1-12.

[xlvi] See Carrier, B. and Spafford, E.H., 2003. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2(2), pp. 1-20.

[xlvii] See Rogers, M., 2006. DSCA: A Practical Approach to Digital Crime Scene Analysis. In Information Security Management Handbook, Fifth Edition, Volume 3. pp. 601–614.

[xlviii]See Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S., 2006. Computer Forensics Field Triage Process Model. In Proceedings of the conference on Digital Forensics, Security and Law (CDFSL 2006). Association of Digital Forensics, Security and Law, p. 27.

[xlix]See Carrier, B. and Spafford, E.H., 2004. An Event-Based Digital Forensic Investigation Framework. In Digital Forensic Research Workshop. pp. 11-13.

[l] See Baryamureeba, V. and Tushabe, F., 2004. The Enhanced Digital Investigation Process Model. In Proceedings of the Fourth Digital Forensic Research Workshop. pp. 1-9.

[li] See https://www.researchgate.net/publication/274273665_Integrated_digital_forensic_process_model, consulted on 31/03/2023 at 2am

[lii] Ibid

[liii]See Palmer, G., 2001. A Road Map for Digital Forensic Research. In First Digital Forensic Research Workshop, Utica, New York. pp. 27-30.

[liv]See Lee, H.C., Palmbach, T. and Miller, M.T., (2001). Henry Lee's Crime Scene Handbook, Academic Press, pp. 1-10.

[lv] See Ciardhuáin, S.Ó., 2004. An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), pp. 1-22.

[lvi] See Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., 2013. Integrated Digital Forensic Process Model. Computers & Security, 38, pp. 103-115.

[lvii] See Carrier, B. and Spafford, E.H., 2004. An Event-Based Digital Forensic Investigation Framework. In Digital Forensic Research Workshop. pp. 11-13.

[lviii] See Baryamureeba, V. and Tushabe, F., 2004. The Enhanced Digital Investigation Process Model. In Proceedings of the Fourth Digital Forensic Research Workshop. pp. 1-9.

[lix] See Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S., 2006. Computer Forensics Field Triage Process Model. In Proceedings of the conference on Digital Forensics, Security and Law (CDFSL 2006). Association of Digital Forensics, Security and Law, p. 27

[lx] See Ciardhuáin, S.Ó., 2004. An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), pp. 1-22.

[lxi]See Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S., 2006. Computer Forensics Field Triage Process Model. In Proceedings of the conference on Digital Forensics, Security and Law (CDFSL 2006). Association of Digital Forensics, Security and Law, p. 27.

[lxii] See Perumal, S., Norwawi, N.M. and Raman, V., Internet of Things (IoT) Digital Forensic Investigation Model: TopDown Forensic Approach Methodology. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, pp. 19–23.

[lxiii] Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., (2011). Systematic Digital Forensic Investigation Model, International Journal of Computer Science and Security (IJCSS), 5(1), pp.118-131.

[lxiv] See Kohn, M.D., Eloff, M.M. and Eloff, J.H.P., 2013. Integrated Digital Forensic Process Model. Computers & Security, supra

[lxv] See Martini, B. and Choo, K.-K.R., 2012. An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Digital Investigation, 9(2), pp.71-80.

[lxvi] See Quick, D. and Choo, K.-K.R., 2014. Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive. Trends and Issues in Crime and Criminal Justice 480(1).

[lxvii]See Perumal, S., Norwawi, N.M. and Raman, V., Internet of Things (IoT) Digital Forensic Investigation Model: TopDown Forensic Approach Methodology. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, pp. 19–23.

[lxviii] See Martini, B. and Choo, K.-K.R., 2012. An Integrated Conceptual Digital Forensic Framework for Cloud Computing. Digital Investigation, 9(2), pp.71–80.

[lxix] See McKemmish, R., 1999. What is Forensic Computing?, Australian Institute of Criminology Canberra.

[lxx]See Quick, D. and Choo, K.-K.R., 2014. Data Reduction and Data Mining Framework for Digital Forensic Evidence: Storage, Intelligence, Review and Archive. Trends and Issues in Crime and Criminal Justice 480(1).

[lxxi] Perumal, S., Norwawi, N.M. and Raman, V., Internet of Things (IoT) Digital Forensic Investigation Model: TopDown Forensic Approach Methodology. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, pp. 19–23.

[lxxii] See Hitchcock, B., Le-Khac, N.-A and Scanlon, M., 2016. Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists. Digital Investigation, 16, pp. S75-S85.

[lxxiii] See https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime, consulted on 30/03/2023 at 10am

[lxxiv] At its simplest, security is the process of protecting against injury or harm. Security also describes the safeguards, or countermeasures, put in place by that process. In computer security, harm implies a loss of desired system properties such as confidentiality, integrity, or availability. The goals of security may be distinguished from those of reliability in that they focus on preventing injury or harm resulting not only from random acts of nature, but also from the intentional strategic actions of those with goals counter to your own.

[lxxv] Virtualisation is the creation of a virtual rather than actual version of something, such as an operating system (OS), a server, a storage device or network resources. Virtualization uses software that simulates hardware functionality to create a virtual system. This practice allows IT organizations to operate multiple operating systems, more than one virtual system and various applications on a single server.

[lxxvi] Schechter, S. (2004). Computer security strength and risk: A quantitative approach. PhD thesis, Harvard University, pp. 9-26.
[lxxvii] See Asongwe, P. 'e-Government and The Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges', supra p.163.
[lxxviii] See Milagros. C., 'Success Factors and Challenges in Digital Forensics for Law Enforcement: A Systematic Literature Review' (LL.M. Thesis, University of Skovde 2021) P.28.