Next Generation Sound Digital Forensics Architecture - A Novel Conceptual Framework
Obwaya Mogire
South Eastern Kenya University
School of Information and Communication Technology
Department of Telecommunications and Information Technology

Abstract
Nothing epitomizes modern life better than the computer. For better or worse, computers have infiltrated every aspect of our society and for millions of people worldwide, the use of computers has become a central part of life. These advances have led to new opportunities, risks and challenges for technical and legal structures. The increase of digital crimes puts a lot of pressure on law enforcement agencies and or organizations across the globe to produce credible digital forensic evidence. This has seen a paradigm shift in the world where there is an increasing need for Digital Forensics (DF). This growth of technology has therefore produced a completely new source of evidence referred to as ‘electronic evidence’. Electronic evidence is fragile and volatile by nature and therefore requires the investigator always to exercise reasonable care during its collection, preservation and analysis to protect its identity and integrity. The purpose of this research was two-fold, to investigate factors that influence digital forensic reliability, admissibility and secondly, to develop a novel digital forensic model for the next generation that will produce authentic and hence admissible e-evidence for legal proceedings. Thorough review of existing literature on digital forensics and forensic models was done and from gaps identified, a novel conceptual model towards sound forensics processes is proposed here. The findings are critical in developing as a guide in providing Digital Forensics services whether internal investigation, disciplinary hearing or court case. Recommendation is that the forensics investigators need to ensure that their evidence meets legal requirements and that their legal professionals are trained in digital forensic procedures. Establish a well-defined forensic policy that will mandate and provides guidelines for forensic investigations, establishment of a digital forensic laboratory and organizations should ensure more effort is given to digital forensics training and awareness.

Keywords: Admissibility, Digital Forensics, Digital Evidence, DF Model

I. INTRODUCTION
Digital forensics is becoming a business enabler but very few organizations have the necessary structures in place to enable them to conduct cost effective, low-impact and efficient digital investigations. The legal requirement is that the collected digital evidence must be relevance, reliability, and authenticity for it to be admissible in any court proceedings. Previous researchers state that the chances of success in criminal prosecution by law enforcement agencies rely heavily on the availability of strong evidence. However, the adoption, proliferation and maturation of digital forensics have been sluggish due to inadequate corporate governance, lack of forensic policies, legal and ethical requirements, as well as improper use of technology and infrastructure. Digital forensics is a new paradigm that is laborious and requires significant expertise on the part of the investigator. The investigation requires defined procedures that comply with industry practices, organizational practices and appropriate laws, whether as part of a criminal investigation or as part of a more general security incident response. According to (Kenneally, 2002) Presenting digital evidence is a unique legal challenge facing digital forensics professionals. Kenneally notes that evidence in legal cases is admitted or threshed based on the relative weight of its probative and prejudicial value. According to (Ryan & Shpanzer, 2002) evidence, to be admissible in court, must be relevant, material and competent, and its probative value must outweigh any prejudicial effect. Digital evidence is not unique with regard to relevancy and materiality, but because it can be easily duplicated and modified, often without leaving any traces. According to (Sommer, 2009) chances of success in criminal prosecution by law enforcement agencies depend heavily on the availability of strong evidence, and failure in civil proceedings means financial loss, because a failed criminal prosecution can generate reputation damage to businesses and organizations leading to huge financial loss. Digital forensics process is more often than not faced with challenges related to admissibility, authenticity, accuracy, relevancy, non-repudiation, reliability, credibility, and completeness due to lack proper corporate governance, forensic policy, legal and ethical requirements, digital forensic laboratory, trained staff , technology and infrastructure . The field of digital forensics is undergoing a rapid metamorphosis. It is changing from skilled craftsmanship into a true forensic science and part of this change is expressed by the interest in this field as an academic study. For the same reason, a more novel forensics model for sound digital forensics processes is required.
II. DIGITAL FORENSICS

There have been several efforts to define and find research areas in Digital forensics. Nikkel (2006) defined Digital Forensics, as the collection, preservation, analysis, and presentation of digital evidence usable for internal disciplinary hearings, digital evidence as a supporting data for internal incident report and digital evidence admissible in the court of law. The term Digital Forensics comprises a wide range of computer activities, not just evidence from computer, e.g. disk drive and computer memory, but including all sorts of generic media, cell phones, memory sticks, PDA’s, network traffic etc. Carrier and Spafford (2006) define Digital Evidence as a digital data that supports or refutes a hypothesis about digital events or the state of digital data. This definition includes evidence that may not be capable of being entered into a court of law, but may have investigative value. Palmer (2001) defined Digital forensic as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. This definition covers the broad aspects of digital forensics from data acquisition to legal action.

III. THE GAP

In the current world where information and knowledge is becoming one of the most sought after commodity; criminals, competitors and even employees exploit loopholes in current security architectures and control structures to obtain the required information for criminal activities. Organizations not only spend a lot of time and money but also effort in planning for incidents, natural disasters or security breaches by drafting incident response, disaster recovery and business continuity plans. These plans identify an incident and prescribe the best way to recover and continue with the business as quickly as possible. However, according to Sommer (2005), very little thought is given to the identification and preservation of digital evidence and the correct structuring of processes for possible prosecution. Sommer points out that very few organizations have the structures in place to enable them to conduct cost effective, low-impact and efficient digital investigations. Often, when asked for specific digital evidence, most organizations do not have all the evidence available (Clark, 2006). Courts no longer require only document-based or witness-based evidence but also electronic-based evidence in this era of ubiquitous and pervasive of digital technology. However according to Ayers and Jansen (2007), Law enforcement and digital forensics still lag behind when it comes to dealing with digital evidence obtained from digital devices. The demand for digital based evidence by courts means the need for proper Digital Forensics is becoming more crucial. According to (Joshi & Bhilare, 2014), DF continue to face a lot of challenges due to the fact that the attack may be initiated at some indeterminate distance from the target, the attacker may have used any of a number of techniques to obfuscate his or her true location or/and can use anti-forensics methods that prevent forensic tools, investigations, and investigators from achieving their goals. Further that in a serious digital incident there can be yottabytes of data that may (or may not) contain even bytes of evidences. Beebe, in 2009 admitted that as an area of future growth and improvement, Digital Forensics largely lacks standardization and processes, and what little widespread knowledge that we have is “heavily biased towards Windows platform, and to a lesser extent, standard Linux distributions.” Beebe elaborated the unaddressed issues of Digital Forensics, highlighting that the problem of scalability, lack of intelligent analytics beyond full-text search that could link up multi part scenarios, non-standard computing devices especially small and hand held devices, ease-of-use, and a laundry list of unmet technical challenges are the work that needs to be addressed in future with new technologies and research.

In 2010, Garfinkle argued in his paper entitled “Digital forensics research: The next 10 years” that we have been in a “Golden Age of Digital Forensics,” and that the Golden Age is quickly coming to an end. Increasingly organizations encounter data that cannot be analysed with today’s tools because of format incompatibilities, encryption, or simply a lack of training. He believes that Digital Forensics is facing a crisis as the result of advances and fundamental changes in the computer industry like the growing size of storage devices, the increasing prevalence of embedded flash storage, the proliferation of operating systems and file formats, pervasive encryption, use of the cloud for remote processing and storage and digital forensic analysis shifted from single device to multiple devices. In 2012 Garfinkle shares his 14 years’ experience in developing DF tools in a paper entitled “Lessons learned writing digital forensics tools and managing a 30TB digital evidence corpus”. In this, he explains that writing digital forensics tools is difficult than other kinds of software because of the diversity of data types that needs to be processed, the need for high performance, the skill set of most users, and the requirement that the software run without crashing. According to (Boddington, Hobbs, Mann, Hobbs, & Mann, 2008), in the past, courts may have been inclined to accept the weight of digital evidence based on expediency and intuition, or if confused by technical issues have dismissed the case out of hand; however, there is the likelihood of increased legal challenges that cast doubt on the weight of the evidence in the future. Further that Digital evidence exists in complex technical environments, unfamiliar territory for most legal practitioners who have difficulty determining how far conventional ideas of evidence can be extended into the digital domain. All organizations should have standards, policies and procedures in place that can assist in such an investigation (Noblett, et al 2000). Standards that are important here are ISO17799 and COBIT. These standards do not cover a forensic investigation, but could be used to aid it. As well as internal standards and policies, there are several legislative measures that support organizations.
attempting to prosecute computer crimes that must be put in place. Further, from the literature findings, more often than not, a lot of research in this area of digital forensics focuses more on investigative processes or stages or phases without focusing on technology, policies, standards, procedures, intelligence, personnel, governance just but a few (Pollitt 1995, Digital Forensic Research Workshop 2001, Reith, Carr and Gunsch 2002, Carrier and Spafford 2003, Carrier 2003, Mocas 2003, Baryamaeeta and Tushabe 2004, Beebe and Clark 2004, Carrier and Spafford 2004, Pollitt 2004, Kent, Chevalier, Grance and Dang 2006, Erbacher, Christensen and Sundberg 2006). Only a few that proposes policies, procedures, technology (Noblett, et al 2000, McCumber 2005). The need to propose an intelligent “Forensic model” for the next generation.

IV. RELATED LITERATURE
There is an old saying that prevention is better than cure. When applied to forensic models this would seem to imply that preparation is the key to conducting a successful forensic investigation. The number of forensic models that have been proposed reveals the complexity of the Digital forensic process. Most focus on either the investigation itself or emphasize a particular stage of the investigation. Kruse and Heiser 2002 DF framework has three basic components (3A’s): acquiring the evidence; authenticating the evidence, and analyzing the data. These components focus on maintaining the integrity of the evidence during the investigation. The United States of America’s Department of Justice proposed a process model for Digital forensics abstracted from technology and has four phases: collection; examination; analysis, and reporting. There is a correlation between the ‘acquiring the evidence’ stage identified by Kruse and Heiser and the ‘collection’ stage proposed here. ‘Analyzing the data’ and ‘analysis’ are the same in both frameworks. Kruse has, however, neglected to include a vital component: reporting. The Scientific Crime Scene Investigation Model proposed by Lee (2001) consists of four steps: recognition; identification; individualization, and reconstruction. These steps all clearly fall within the ‘investigation’ stage of the process; there is neither a ‘preparation’ nor ‘presentation’ stage either side. Casey (2000) proposes a framework similar to Lee. This framework focuses on processing and examining digital evidence. The steps included are: recognition; preservation; classification, and reconstruction. In both Lee and Casey’s models, the first and last steps are identical. Casey also places the focus of the forensic process on the investigation itself. The Digital Forensics Research Working Group (DFRW, Palmer, 2001) developed a framework with the following steps: identification; preservation; collection; examination; analysis; presentation, and decision. This framework puts in place an important foundation for future work and includes two crucial stages of the investigation. Components of an investigation stage as well as presentation stage are present. Reith, Carr and Gunsch (2002) proposed a framework that includes a number of components that are not mentioned in the above frameworks. The full listed components are: identification; preparation; approach; strategy; preservation; collection; examination; analysis; presentation, and returning evidence. This comprehensive process offers a number of advantages, as listed by the authors. The model proposed by Ciardhuáin (2004) is probably the most complete to date. The steps or phases are also called ‘activities’. The model includes the following activities: awareness; authorization; planning; notification; search for and identify evidence; collection; transportation; storage; examination; hypothesis; presentation; proof/defense, and dissemination. Seamus model (2009) is the most latest and covered quite number of process. The model includes the following activities such as planning, identification, reconnaissance, analysis, result, proof and defense, and archive storages. Planning stage includes authorization by obtaining search warrant. Reconnaissance involves gathering evidence, transport and storage. (Ami-narh & Williams, 2008), Digital Forensics and the Legal System Model; identification/preparation, search and seizure of evidence, preservation of evidence, examination, analysis and reporting. Documentation takes place in the entire activities. According to Sommer (2008), Digital Forensics framework has three dimensions as shown below; People, Technology and Processes. This framework captures a very important aspect of DF. Digital forensics should be integrated into the discipline of information assurance as one of its methods. According to McCumber (2005), the security countermeasures are the technologies, policies, practices and human factors (training, vetting employees, etc.) that implement information assurance. These countermeasures are deployed through the three basic information pillars:-transmission, storage and processing; providing three services to system:-Confidentiality, Integrity and Availability. He argues that digital forensics has a function within each cell of the cube (Fig.1), giving it a role in enterprise information systems operations. Thus defining what it means for a country to be “forensically ready” incorporates the full spectrum of information assurance (IA) elements:-security, policies, procedures, practices, mechanisms, and security awareness training programs.

Fig. 1 Dimensions of Integrated Digital Forensics in Information Assurance (McCumber, 2005).

From the proposed frameworks mentioned above, it’s clear that each of the proposed models builds on the experience of
the previous. Some of the models have similar approaches and some focus on different areas of the investigation. Perhaps the best way to balance the process is to ensure the focus remains on achieving the overriding goal of producing concrete evidence suitable for presentation in a court of law. This is the goal of this research and integrating all models to produce a more novel model that befits the next generation.

V. PROPOSED NOVEL DF MODEL

The previous section outlined several important forensic frameworks. In this section a new framework will be proposed. The aim is to merge the existing frameworks already mentioned to compile a reasonably complete DF framework. According to Sommer (2008) & McCumber (2005), a good DF framework has three basic components namely people, technology, and process. Noblett, et al 2000, focuses organizational policy and practices, procedures and techniques. Together with models proposed by (Pollitt 1995, Digital Forensic Research Workshop 2001, Reith, Carr and Gunsch 2002, Carrier and Spafford 2003, Carrier 2003, Mocas 2003, Baryamueeba and Tushabe 2004, Beebe and Clark 2004, Carrier and Spafford 2004, Pollitt 2004, Kent, Chevalier, Grance and Dang 2006, Erbacher, Christensen and Sundberg 2006), we must ensure e-evidence is authentic, reliable, accurate, relevant, complete, and credible so as to be admissible before a court. We combined these research findings and by taking Sommer (2008), McCumber (2005), Noblett, et al 2000, and the U.S.A model (undated). They both agree on technology, regulatory policies and processes. We therefore take technology, policies and processes as the key dimensions of any DF model. These however must be resultant of some interaction of some other dimensions, like governance, training and people (Noblett, et al 2000, McCumber, 2005). Since technology, policies and governance is one of the challenges DF faces, we are of the view that DF must have other pillars to support them if they are to be successful. This is where we make reference to the other models discussed above. We advanced a proposition that technology, policies and processes are the dimensions whose interplay determines the governance, training, staff on DF. The admissibility, authenticity, credibility, accuracy, relevance, reliability and completeness of digital evidence of a DF process is then determined by these six dimensions as referenced from Gordon (2006) through proper DFI processes as outlined by both (Ciardhuáin, S. O. 2004) and (IJCNSN 2009). This is diagrammatically represented in Fig 2. In our novel framework, DF is creation of interplay between six dimensions. We have however categorized them into two. One category comprise of technology, regulation and processes. These dimensions must be backed by the second category namely governance, training and people. It is from such components that will yield the admissibility, authenticity, credibility, accuracy, relevance, reliability and completeness of digital evidence through proper phases of DF. Table 1. Shows a number of other related framework from which the proposed framework references.

Table 1. Various DF models reviewed

<table>
<thead>
<tr>
<th>Model Name</th>
<th>Inventors</th>
<th>Years</th>
<th>Number of Stages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Forensic Process</td>
<td>M.Pollitt</td>
<td>1995</td>
<td>4 Stages</td>
</tr>
<tr>
<td>Generic Investigation Process</td>
<td>Palmer</td>
<td>2001</td>
<td>7 Stages</td>
</tr>
<tr>
<td>Abstract Model of the Digital Forensic Procedures</td>
<td>Reith, Carr, &amp; Gunsch</td>
<td>2002</td>
<td>9 Stages</td>
</tr>
<tr>
<td>An Integrated Digital Investigation Process</td>
<td>Carrier &amp; Spafford</td>
<td>2003</td>
<td>15 Stages</td>
</tr>
<tr>
<td>End To End Digital Investigation</td>
<td>Sophokleous</td>
<td>2003</td>
<td>9 Stages</td>
</tr>
<tr>
<td>Enhance Integrated Digital Investigation Process</td>
<td>Baryamueeba &amp; Tushabe</td>
<td>2004</td>
<td>25 Stages</td>
</tr>
<tr>
<td>Essential Model of Cyber Crime Investigation</td>
<td>Curtin</td>
<td>2004</td>
<td>13 Stages</td>
</tr>
<tr>
<td>Hierarchical Object Based Framework</td>
<td>Beebe &amp; Clark</td>
<td>2004</td>
<td>6 Stages</td>
</tr>
<tr>
<td>Event Based Digital Forensic Investigation Framework</td>
<td>Carrier &amp; Spafford</td>
<td>2004</td>
<td>16 Stages</td>
</tr>
<tr>
<td>Forensic Process</td>
<td>Kent K. Chevalier, Grance, &amp; Dang</td>
<td>2006</td>
<td>4 Stages</td>
</tr>
<tr>
<td>Investigation Framework</td>
<td>Kehrs, Hoff &amp; Oliver</td>
<td>2006</td>
<td>3 Stages</td>
</tr>
<tr>
<td>Computer Forensic Field Tracing Process Model</td>
<td>K.Roger,Goldman,Milan,Wedge &amp; Debes</td>
<td>2006</td>
<td>4 Stages</td>
</tr>
<tr>
<td>Investigation Process model</td>
<td>Freiling &amp; Schottky</td>
<td>2007</td>
<td>4Stages</td>
</tr>
</tbody>
</table>

Fig.2: The Proposed DF framework

COMPONENTS OF FRAMEWORK

A. Technology

No DF investigation can be conducted without a DF toolkit. Various specialized software and/or physical hardware tools will make up the DF toolkit as different tools are used for different purposes. The ways in which the tools are utilized as well as the acceptance of a specific tool by the legal authorities are vital for any forensic investigation. Although courts have found that an inanimate object, e.g. a software package cannot be considered to be an expert, the results generated by an acceptable software package are acceptable. The person who will use the software packages will have to be an expert.

B. Policy

Every organization needs policies to guide employees on activities. A general forensic investigation policy is required to provide a framework for DF policies in the organization. Examples of other policies are how to handle evidence, how to seize evidence and how to conduct covert or overt
investigations. Policies are normally supported by procedures and guidelines. Procedures also need to be set up so that the investigations will be able to stand up to legal scrutiny in court. These procedures must also be scientifically sound and proven to maintain the integrity of the evidence and process. Yasinsac and Manzano (in Rawlingson, 2004) note that enterprise policies can enhance computer and network forensics.

They propose six categories of policies to facilitate Digital Forensic Investigations (DFI) i.e. retaining information, planning response, training, accelerating investigation, protecting evidence and preventing anonymous activities. Well-defined policies give digital investigations and forensic examiners the authority to carry out investigations in the organization. Policies will demonstrate that an organization intends to be fair-minded and objective about how it treats employees and that it will follow due process for all investigations. The Legal and Ethical are part of policies and are very important in organizations. In Cyberspace there is no universal or common ‘Cyber law’. Various judiciary systems exist in different countries. The forensic investigator must be conversant with local legal and international laws, treaty requirements and industry specific legal requirements when preparing to present a case that will be able to stand up to legal scrutiny in court. The ethical aspect of DF is becoming more and more important. Although the Legal and Ethical aspects of DF have been placed together in the same dimension, it is essential to note that not all legal operations or actions are ethical. It is essential that the DF investigator does not abuse the trust that the employees place in him / her. DF investigator utilizes tools that, if handled inappropriately, can cause a lot of damage in an organization. There should be very clear guidelines on moral behavior and possibly a code of conduct for DF Investigators to guide professional behavior.

C. Processes

According to the proposed definition, these activities are investigative in nature, and those practitioners who will employ these tools and methods will follow some form of investigative process in the performance of their duties. If properly categorized, the processes can enable practitioners to visualize where they need to add capability from what is available. Likewise, academic researchers will use the process to look for shortfalls in technology, helping them to focus on areas where research is needed the most.

D. Governance

The Corporate Governance dimension will handle the management aspects of DF in an organization. Management is responsible for the security posture of an organization. Management can only manage security incidents if for example the root cause of the event is determined and appropriate action to rectify it can be taken – this may involve forensic investigations. According to Von Solms and Louwrens (2005), IT Governance is a subset of Corporate Governance and Information Security Governance a subset of IT Governance. DF overlaps with Information Security Governance, IT governance and Corporate Governance (Von Solms & Louwrens, 2005). Forensic readiness will help to demonstrate due diligence and good corporate governance of an organization’s assets (Rawlingson, 2004). It is therefore imperative that a forensic investigation must be performed in a way that it adds value and improves the security posture of an organization. The Corporate Governance dimension includes strategic governance and operational governance. Typically strategic governance will be from a strategic perspective, while operational governance will provide management directives on an operational level.

It is vital that management should become involved and buy into the DFMM of the organization. DF investigations can be very expensive and management must realize the need for investigations, as well as dealing with the results from an investigation. The operational governance dimension should guide the management on how to manage digital forensic investigations by providing a DFMM. This DFMM must include reactive DF as well as pro-active DF management. Pro-active DF management must ensure that all business processes are structured in such a way that essential data and evidence will be retained to ensure successful DF investigations, should an incident take place. Proper pro-active DF management should minimize interruption to the business processes while conducting an investigation. It is essential that the organization become DF prepared. Re-active DF management should clearly define the management or process of an investigation, once an incident has occurred.

E. People

People are the most important part of any organization and normally the weakest link in the security chain of the organization. When an incident occurs it is most likely that people will contaminate the evidence while figuring out what has happened. Training is therefore essential. According to Rawlingson (2004) there is a gigantic need for forensic awareness training. This dimension will look at training and awareness programs in an organization. The profile and composition of a DF team is also very important. One person normally does not have all the required skills to conduct an investigation. It is important that digital forensics units uphold skilled, competent examiners. This can be accomplished by developing the skills of existing personnel or hiring individuals from specific disciplines. Because of the dynamic nature of the field, a comprehensive ongoing training plan should be developed based on currently available training resources and should be considered in budget submissions. Consideration may also be given to mentor programs, on-the-job training, and other forms of career development. Professional organizations such as the Information Systems Audit and Control Association (ISACA), the High Technology Crime Investigation Association (HTCIA), the Institute of Internal

Auditors (IIA), the Association of Certified Fraud Examiners (ACFE) and the Information Systems Security Association (ISSA) have offered training support in this evolving area. The specialists are trained extensively on knowledge of software packages and utilities used to obtain data.

Individuals must go through rigorous training and have a firm working knowledge of the software to be competent enough to pass the test. Digital forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating. This can be attained by constructing a comprehensive training program for examiners, sound digital evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency.

F. Training

It is good practice to have a dedicated internal organization or staff capacity to undertake digital evidence scrutiny. Forensics training and awareness-on new technologies (tools, processes, governance, Processes-recovery, analysis, examination and presentation of e-evidence) is paramount. It is good practice to give special training to the agency’s staff who are involved in DF processes. Computer forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating.

VI.VALIDATING DF FRAMEWOK

(Arbuckle 2005) mentions that model evaluation is one of the most difficult and unsettle issues related to structural equation modeling. In this research the model is validated using confirmatory factor analysis (CFA). The CFA is carried out using Structural equation modeling (SEM software Analysis of Moment Structures (AMOS 16). The objective of the CFA is to construct a structural model which aligns the tested measures to the specific constructs, by constraining the variance of each measure to the specific latent construct it should represent. In addition to assess the degree to which each measure contributes to its latent construct, the CFA also tests the separation between constructs by evaluating the fit in the overall model. The fit measures within each group give the same rank of ordering of models. Figure 3. Represents the result of testing the structural links of the research model using AMOS 16. The estimated path coefficients are given along with the standardized regression weights. Structural equation modeling is well suited to test a group of constructs simultaneously in the form of a model with significant level 0.05. Together with chi-square and degree of freedom all lie within the recommended values. It helps to reveal these hypotheses and to consider each one individually.

VII.DISCUSSION AND CONCLUSIONS

As challenging as the profession of digital forensics has been to date, still more interesting problems are looming on the horizon. Computers are proliferating throughout modern society. Once we gathered digital evidence from monolithic, stand alone mainframes, Today we have PC’s, supercomputers, distributed client-server networks, laptops, palmtops, and PDA’s, all of which can, and do, provide digital evidence at times. We have networks that use twisted pairs, coaxial cables, fiber optic cables, radio, and infrared radiation to convey information. We have LAN’s and WAN’s. Digital evidence stored in one computer is readily available to a miscreant using another computer half a world, and several legal jurisdictions, away.

As computers become smaller, faster and cheaper, computers are increasingly embedded inside of other larger systems in ways that are not always obvious and allow information to be created, stored, processed and communicated in ways that are unprecedented. Consequently, digital evidence can arise in unexpected places and forms. Instrumentation of spaces for every purpose from environmental monitoring to interactive control of heart rhythms will mean that digital evidence will be even more difficult to collect and analyze.

Computerized control systems manage banks, factories, retail inventories, air traffic control, hospitals, schools, corporations, and government organizations. Computers and their software programs are embedded in our cars, boats, trains and planes, in tools, equipment, and machinery, in telecommunications systems and public switched networks, even in our bodies. Each of them is a potential source of digital evidence, the collection, storage, analysis, and presentation of which is and will be constrained by evolving legal standards and constraints that we fail to understand at our peril. Digital evidence are presented, examined, and challenged by the jury and the judges in the courtroom. The
digital revolution has created the need for new laws, computer forensic investigators, forensic methods, forensic tools and techniques. The framework presented in Figure 2 has six constructs that were found to significantly influence the admissibility of digital evidence. The framework is generic and can be used in any country. Further research is needed since Digital Forensics is still young and in its tender stages-meaning research in the area is still scanty.

**VIII. REFERENCE**


