Davies G and Smith K, J Forensic Leg Investig Sci 2019, 5: 027
DOI: 10.24966/FLIS-733X/100027

HSOA Journal of Forensic, Legal & Investigative Sciences

Research Article

# The Feasibility of Creating a Universal Digital Forensics Framework

**Gareth Davies* and Kim Smith**

*Department of Engineering and Science, Faculty of Computer, University of South Wales, UK*

## Abstract

The aim of this paper was to identify quality evidence that supports the feasibility that a standardized digital forensic methodology for all investigations of all digital artifacts in the global environment can be generated. The industry acknowledges that the current methodologies are not adequate for the needs of the fast-changing environment of digital forensics, and a key driver will be the development of the reputation of digital forensics as a field of science. Alongside this will be the global acceptance of standard legislation that will deal with cyber-crimes in an unbiased judicious manner. The result of this research is that it is feasible to generate a global standard for digital forensic investigations if organizations work together.

**Keywords:** Digital evidence; Digital forensics; Methodologies; Standardization; Universal framework

## Introduction

In this research, we address several different objectives that make up the whole aim. The following are the objectives for this research:

- To identify the justifications for a standard in the subject area of digital forensics
- To identify the barriers to a global standard
- To be able to make recommendations on how to create a single global digital forensics standard

The field of digital forensics has been expanding at an exponential rate and continues to develop quickly, it is falling behind the technological developments; however, it is not as far behind as the legal system throughout the world. The reason for this increase is the need to investigate digital evidence which is generated in all criminal activity. Rob Altoe [1] in 'Digital Forensics in an eDiscovery World' discusses this and highlights that each artifact that is discovered needs analysis, poses its own unique challenges as no two will be the same.

Added to the complexity of digital forensics is the impact of remote and distributed systems as well as the developing technology of artificial intelligence (AI). The challenge is to present evidence with a reliable method; with such a variety of methods a key area for development is the standardization to meet all current and future requirements. This research will concentrate on the current models utilized by investigators and will investigate the analysis already performed to standardize the methods. The sources for this information will be specialist journals such as International Journal of Digital Evidence and articles found on forensic websites, as well as academic books on the subject.

In his book 'Digital Forensics Threats cape and Best Practices' John Sammons [2] put together several expert authors to write about specific areas. Mark Pollitt was one of the contributors and he introduced the simplest digital forensics model, the 4-stage model (Figure 1) developed in 2006 by the National Institute of Standards and Technology (NIST).


**Figure 1:** National Institute of Standards and Technology (USA) model.

As well as providing an outline of a model he also clearly defines the goals of digital forensic investigation. This is a good start point for any future standard, in understanding the foundation of the role and building from that.

His two goals were:

- To preserve the integrity of the evidence
- To find and make available information of value to the submitter of the evidence.

There have been multiple studies carried out on standardization of a digital forensic investigation model; many comparisons have been undertaken by various specialists from academic studies to organization procedural development.

## Research Methods

The fluid environment of digital forensics increases the opportunity for inadmissibility of evidence, a reputation for sound scientific method must be established as it has with other sciences. An example being fingerprinting which was not introduced into criminal proceedings until 1901 [3] when they were accepted by Scotland Yard as a

***Corresponding author:** Gareth Davies, Department of Engineering and Science, Faculty of Computer, University of South Wales, UK, Email: gareth.davies@southwales.ac.uk

**Citation:** Davies G, Smith K (2019) The Feasibility of Creating a Universal Digital Forensics Framework. Forensic Leg Investig Sci 5 : 027.

**Received:** June 03, 2019; **Accepted:** July 16, 2019; **Published:** July 23, 2019

valid method to identify an individual. They are now an accepted and common method for identification of individuals in criminal cases.

It is hoped that the output of this research will be an understanding and a consensus that a standardized model is required and initiating collaboration between nations across the world to achieve this common goal.

Previous studies of digital forensic methodologies have concentrated on a comparison of what exists and how to improve what exists to make the process more reliable, and thus generate a new methodology. In this project, the aim was different; the intention was to review the comparison literature that exists on digital forensics and develop an understanding of what is the purpose of the investigation methodology. Simultaneously, a review of current trends in Information Technology and the future possible infrastructure changes that may cause barriers for evidence gathering was performed.

## Standards

It is important that a standard model is developed, and a definition of a standard must precede this. Below I have proposed a definition of a standard for digital forensic investigations.

A standard is a structured set of rules, guidelines or characteristics that are a measure of the quality and provide an assurance of the fitness for purpose of an output from a human endeavor. This set of rules, guidelines and characteristics will have been generated from a consensus of experts in the subject field.

Considering the development cycle of the field of digital forensics and the stage that it has currently reached it can be implied that the next stage will be to support the development of automatic processes which would allow for the larger volumes of evidence that are retrieved to be processed more effectively and efficiently. The digital forensic industry is ready for this next stage of evolution.

There are both advantages and disadvantages to the implementation of standards within the industry. The following are some common advantages to standardization:

- Provide a definition of common technological terms
- Allows for individuals to train to the same level of knowledge and expertise
- Ensures that the industry has integrity
- Give confidence to the consumer
- Updated regularly to keep pace with technology
- Ensure that evidence is not mishandled

### Standards linked to Digital Forensics

Although there is no one standard to cover all activities within the field of digital forensics, there has been an attempt in recent years to create some standards, ISO has made a start on a group of standards known as the ISO27k series to support Information Technology Security. There are four specific ISO standards that are especially important in this specialist area:

ISO17025 – General Requirements for the Competence of Testing and Calibration Laboratories

ISO27035 – Information Security Incident Management

ISO27037 – Identification, Collection, Acquisition and Preservation of Digital Evidence

ISO9001 – Quality Management Systems

### ISO 17025

This standard relates to the issue of reliability of analysis, in that it is concerned with the competence of all laboratories not just those that undertake digital forensics. The purpose is to give members of the public the confidence in the output reports from the laboratories and to give confidence to the courts that any results have been scientifically tested, are impartial and consistent and that results are valid. ISO 17025 is a standard that all laboratories should be trying to gain accreditation to, it was initially timetabled that all laboratories should have gained accreditation by October 2017. However, there has been a low take-up of the accreditation, the current requirement to attain ISO17025 is costly and time consuming, and this is a barrier. The standard has been written in such a way as to provide some instruction; guidance on the development of a laboratory and its structure as well as the equipment that would be expected to be in existence to provide the consistent reliability of testing, however it does not fully support a standard methodology for digital forensic investigations.

## Discussion

### An examination of digital forensic models International Journal of Digital Evidence

In this comparison, the authors [4] have compared four models, this being one of the first comparisons to be performed on models discusses those that are widely used at this time. Early on in this paper the authors clearly understood the importance of being able to have a consistent and well-defined method to use and that standardization was the best way forward.

The authors discuss the reasons why no standard had been developed realizing that current models were based on the technology available and were very ad-hoc. These developments have been inspired by the emergence of new technology and the need to be able to analyse data, not from the scientific community, and therefore they are not considered to be reliable and are untrusted in a court of law.

### The four models that were discussed were:

- Farmer and Venema [5] 5 steps to dealing with a situation
- K Mandia and C Prosise Incident response methodology
- Department of Justice model
- DFRWS model

The authors [6] developed a model that was the Abstract Digital Forensic Model (Figure 2) and was generated from the commonality of the other four models; this evolution of models appears to follow the same process all the way through its progression. This new model has the advantage that it was based more closely on the traditional investigative techniques used by other forensic fields and therefore should have been more widely accepted as scientific and reliable.

The method is adaptable in its design to permit additional sub-procedures which would support the different classes of digital technology under this model. This would mean that only new sub-procedure Would need to be developed for a new technology, rather than writing a completely new method as is the current trend.

## Taxonomy of Computer forensics methodologies and procedures for digital evidence seizure

In this article [7] the author begins with the basic premise that for every investigation there are three aims:

- Acquire evidence without altering or damaging it
- To authenticate that the copy is the same as the evidence seized
- Analyse the data without altering it.

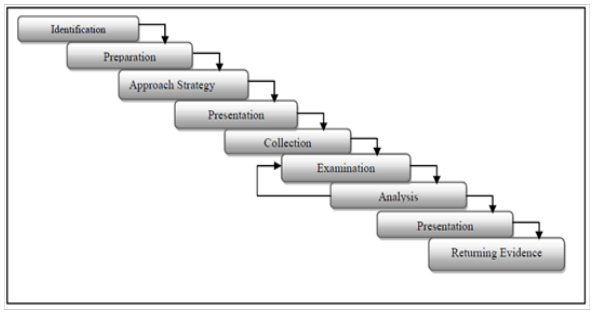


**Figure 2:** Abstract digital forensic model.

This confirms John Sammons two aims of digital forensics. The emphasis of this paper is the European Union Cyber Tools on Line Search for Evidence (CTOSE) (Figure- 3) project and the analysis of the basic steps indicate a five-stage model. This model in its design allows for investigators to undertake work following an iterative process.


**Figure 3:** Cyber tools on line search for evidence model.

The article compares three different methodologies, the Basic Forensics Model, the Cyber Tools On-line Search for Evidence (CTOSE) and Data Recovery UK (DRUK). The comparison is provided in the form of tables for the Identification, Acquisition, Analysis and Reporting phases. The tasks are based upon the author's opinion of what needs to be performed and the article being written in 2006 makes no reference to technology and thus has an advantage that it is generic. It is recognized by the authors that there is a wide diversity of methodologies utilized in digital forensics, but all commonly attempt to provide the same integrity of data. It continues emphasizing that work is needed to provide a standard method for all, that is should be mandatory and a legal requirement which would provide the integrity and reliability that is necessary.

## Common phases of computer forensics investigation models

The comparison was an extensive [8] piece of research and compared 15 models, some of which were discussed in the article by Reith. The main aim of this research was to generate a common model and was justified in its recognition that there were many models that were being used and this was causing issues of admissibility. The outcome of the comparison was the description of a new generic model known as the Generic Computer Forensics Investigation Model (GCFIM).

This research was searching to identify the common phases that went across the majority of models; the authors had to make assumptions about similar phraseology linking similar steps. This needs detailed knowledge of all the methodologies to ensure that a phase is not misinterpreted. The authors were able to generically group activities together and came up with a 5-stage model, the result being the Generic Computer Forensics Investigation Model (Figure 4).

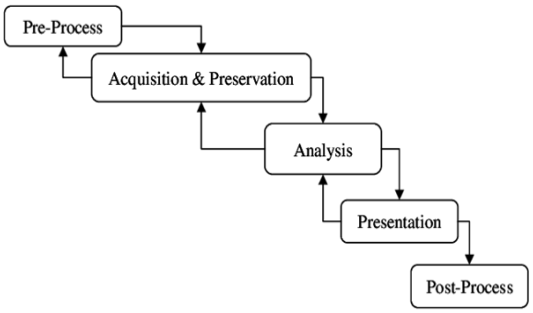


**Figure 4:** Generic computer forensic investigation model.

This model was generated from sound scientific analysis, but the analysis lacks consideration of models generated for other digital devices such as mobile phones. This raises the question of whether this model would be generic enough to consider all digital devices. The authors recognized that the process of digital investigation is not a linear one, which allows for investigators uncovering new leads as they analyse evidence and returning to the data gathering stage.

## Analyses of the state-of-the-art digital forensic investigation process models

In this article the authors [9] recognized the importance of the development of a standardized or harmonized method, and they identified the same common key barriers of jurisdictional boundaries, disparities between number of phases in models, the language and terminology used to identify phases. This analysis had an aim that differed from others, the authors wished to concentrate on the characteristics of the model to highlight the commonality, the difference and those areas where the model could be standardized. The authors mapped all the phases of the models (Figure 5) that they had chosen, this mapping as well as the phases, unconventionally included an analysis of the actionable principles, those actions that need to take place during a digital forensic investigation.

This analysis shows a scientific methodology has been applied to determining the common phases of models. However, the limitation is that this does not consider models for all types of digital devices e.g. Smart phones. In the current Information Technology environment this is a very important element of any discussion on methodologies for digital forensic investigations. The comparison in providing the actionable principles is an important piece of work, it reflects directly the admissibility of evidence and the actions that must be taken by investigators to ensure evidence is admissible [10].

## Comparative Analysis of digital forensic models

This article provides a well-structured analysis (Figure 6) of previous comparisons of digital forensic models [11]. This comparison is concerned with what exists and identifying the elements that are common. If elements are common amongst these models, then it has

been implied that it has been recognized as best practice. This article discusses seven models, in general, this article confirms that there are four main phases of digital evidence investigation i.e. Collection, Examination, Analysis and Reporting.

This analysis shows a scientific methodology has been applied to determining the common phases of models. However, the limitation is that this does not consider models for all types of digital devices e.g. Smart phones. In the current Information Technology environment this is a very important element of any discussion on methodologies for digital forensic investigations. The comparison in providing the actionable principles is an important piece of work, it reflects directly the admissibility of evidence and the actions that must be taken by investigators to ensure evidence is admissible [10].

| | Reference phases | DFWRS [4] | Reith et al. [10] | DOJ [11] | Carrier at al.[12] | Mandia et al. [14] | Beebe et al. [15] | Cuardhuain [16] | Cohen [17] | Casey & Rose [18] | ACPO[6] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Phases** | | | | | | | | | | | |
| 1 | 1. Incident Detection | 1.Identification | 1.Identification | | 2. Detection and Notification | 2.Detection of the incident<br>3. Initial Response | 2.Incident response | 1. Awareness | | | |
| 2 | First Response | | | | | 3.Initial response | 2. Incident response | | | | 2.1 Secure and control the crime scene |
| 3 | Planning | | 3. Approach strategy | | 3. Readiness group of phases | 4. Response strategy formulation | 1. Preparation | | | | 1.Preparations for investigations |
| 4 | Preparation | | 2.Preparation | 1.Preparation | 3. Readiness group of phases | 1.pre incident preparation | | 3.Planning | | | 1.Preparations for investigations |
| 5 | Incident scene documentation | | | 3. Documentaiton of the crime scene | 4.3 document evidence and scene<br>2.4 attaching exhibit labels | | | | | | 2.1 photograph and document the scene |
| 6 | Evidence identification | | 6.examination | 2.recognition and identification | 4.2 survey for digital evidence | | | 5. search for and identify evidence | 1. Identification | 1. Gather information and make observations | 5.1 The collection phase |
| 7 | Evidence collection | 2. preservation<br>3. collection | 4. preservation<br>5. collection | 4. collection and preservation | 4.1 preservation of digital crime scene | 5. duplication<br>7.secure measure implementation<br>8.network monitoring | 3. Data collection | 6. collection of evidence | 2. collection<br>3. preservation | 1. Gather information and make observations | 2.3 Initial collection of volatile data<br>5.1 the collection phase |
| 8 | Evidence transportation | | | 5.packaging and transportation | | | | 7.transport of evidence | 4.transportation | | 3. Transport |
| 9 | Evidence storage | | | | | | | 8.storage of evidence | 5.storage | | 4. Storage |
| 10 | Evidence analysis | 4.examination<br>5. analysis | 7.analysis | 6.examination<br>7. analysis | 4.4 search for digital evidence<br>4.5 digital crime scene reconstruction | 6. investigation | 4. Data analysis | 9. examination of evidence<br>10. hypothesis | 6. Analysis<br>7. Interpretation<br>8.Attribution<br>9. reconstruction | 2. Form a hypothesis to explain observations<br>3. Evaluate the hypothesis<br>4.Draw conclusions and communicate finding | 5.2 The analyses<br>5.3 The examination<br>5.4 The reporting |
| 11 | Presentation | 6.presentation | 8.presentation | 8.report | 4.6 presentation of digital science theory | 10.Reporting | 5. Findings presentation | 11. Presentation of hypothesis<br>12. Proof/ defence of hypothesis | 10. Presentation | 4. Draw conclusions and communicate findings | |
| 12 | Conclusions | 7. decisions | 9.Returning evidence | | | 9. recovery<br>11. Follow-up | 6. Closure | 13. Dissemination of information | 11. Destruction | | 6.Disclosure |
| **Actionable Principles** | | | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Interaction with physical investigation | | | 3. physical crime scene investigation group of phases | | | | | | As principle and set of actions |
| 2 | Preserving chain of evidence | Present | Present | Present | Present | Present | Present | Present | Present | Present |
| 3 | Preserving evidence | Present | Present | Present | Present | Present | Present | Present | Present | Present |
| 4 | Information Flow | | | | | | | Present | | Present |
| 5 | Documentation | Present | Present | Present | Present | Present | Present | Present | Present | Present |
| 6 | Obtaining Authorisation | | | 2. Confirmation and authorisation | | | | Present | | Present |

**Figure 5:** Comparison of digital forensic process models.

| Steps | NIJ | DOJ | DRFWS | Abstract | IDIP | EIDIP | SRDFIM |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| Collection | X | X | X | X | X | X | X |
| Examination | X | X | X | X | | | X |
| Analysis | X | X | X | X | | | X |
| Reporting | X | X | | | | | X |
| Preparation | | X | | X | | | X |
| Approach Strategy | | | | X | | | |
| Preservation | | | X | X | X | X | X |
| Presentation | | | X | X | X | X | X |
| Identification | | | X | X | | | X |
| Return Evidence | | | | X | | | |
| Decision | | | X | | | | |
| Review | | | | | X | X | X |
| Reconstruction | | | | | X | X | |
| Documentation | | | | | X | X | X |
| Authorisation | | | | | X | X | X |
| Survey | | | | | X | X | |
| Traceback | | | | | | X | |
| Dynamite | | | | | | X | |
| Communication | | | | | | | X |
| Exploratory Testing | | | | | | | X |

**Figure 6:** Comparison of digital forensic process models.

However, the aim of a standard methodology is to consider all phases of an investigation not just the phase of extraction and analysis which is missing from this analysis.

## A new digital investigation framework comparison method

This article was a comparative study made on the International scene, [12] the aim of the study is to identify a method that is reliable and has integrity. The articles emphasis is on the phases of the different models and the discovery of four main criteria (Figure 7) i.e. shorter time periods, transparency and privacy of evidence, reliability and consistency and reusability.

These four key criteria can be seen to reflect part of the APCO [13] principles. This analysis is different because it is focused on tasks that should happen for evidence to be admissible in court. The article proposes a new model which does offer an iterative approach which is essential in digital forensic investigations. The model is designed with two outputs:

- The preservation of the evidence - this is essential in a court of law
- The expert witness statements

This is an alternative perspective of the situation and has the benefit of concentrating on the two elements that match to the key strategy of standardization and the aims as described by John Sammons in his book. There is a potential issue with this model, although some stages are iterative not all are. A stage that is not is Collection; the ability to return and retrieve more evidence is of importance in network and distributed systems where it may not be possible to capture all the evidence on the first visit because of the large volumes of data.

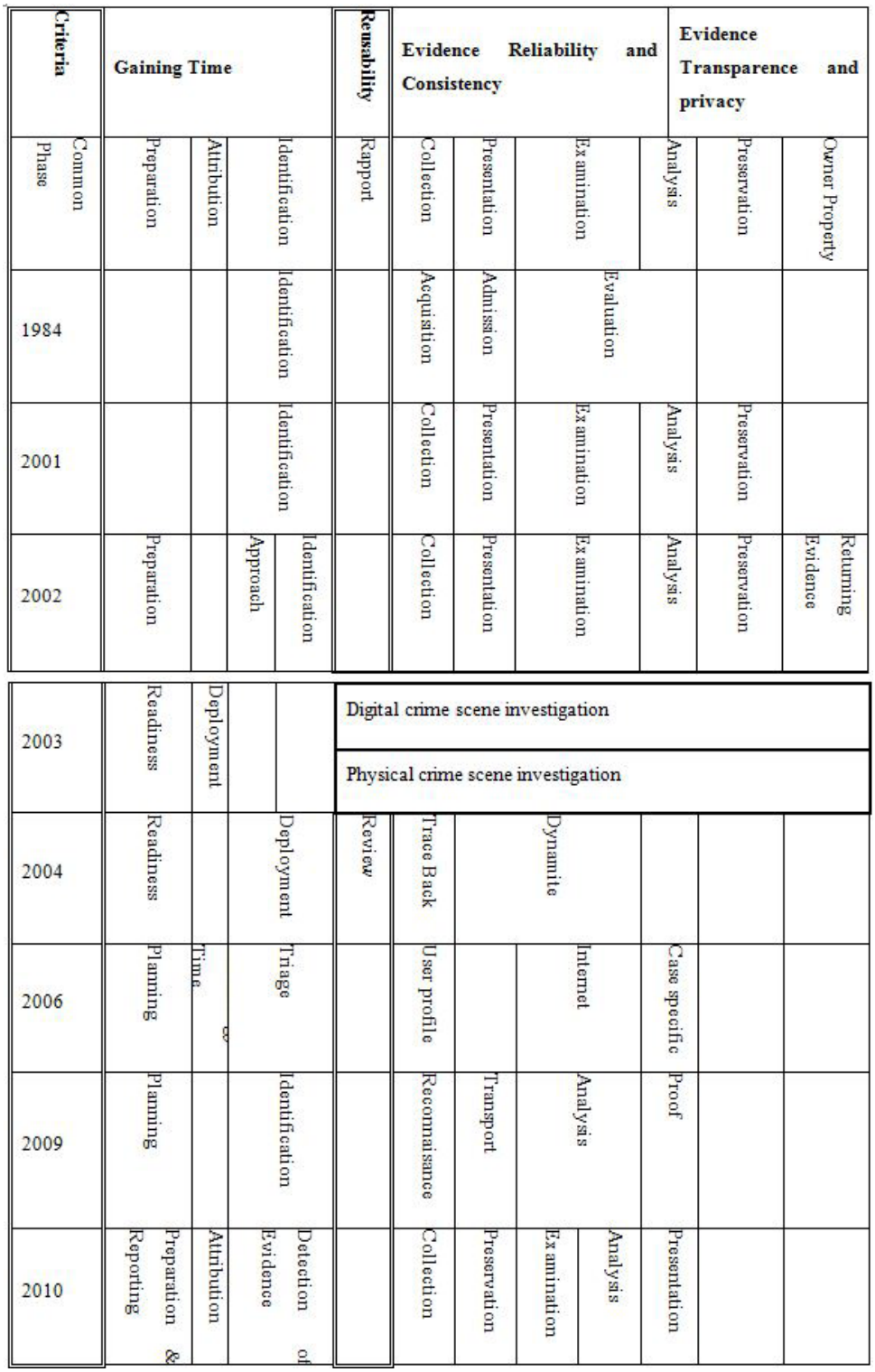


**Figure 7:** Comparative digital investigation model based on respecting criteria.

### Commonality of conclusions

The outcome of the previous studies is generally a proposed new model, one that has been developed from the parts of the existing models. The studies also conclude that a standard model is required, due to the ad-hoc nature of the development of existing models and the fluid environment that digital forensics work in. The science is still evolving at a very fast pace and trying to keep up with the technological changes. Although it is agreed that this is important and that there is a consensus on the need of a standard as well as the basic function of the standard, there is no focus from any formal group to develop this. This review has been developed to identify the commonality of results in the current articles that have been written comparing digital forensic methodologies.

## Barriers

It is evident from the research on digital forensics standardization that there are barriers or challenges to be overcome before a global standard can be adopted. It is not clear whether all these challenges can be overcome and if they can't, can they be tolerated as a risk. In his book Eoghan Casey discusses the impact of admissibility of evidence in court cases. A consideration for a move to standardization is the development of a scientific method increasing the probability of admissibility. Admissibility is the courts determination as to whether evidence is "safe" to put before a jury and will help provide a solid foundation for decisions in the case. In practice, admissibility is a set of legal tests carried out by a judge to assess an item of evidence. This assessment process can become complicated, particularly when the evidence is not handled properly or has traits that make it less reliable or more prejudicial. Some jurisdictions have rules relating to admissibility that are formal and sometimes inflexible, while other jurisdictions give judges more discretion. Some key tests for admissibility are:

- Relevance
- Authenticity
- Not hearsay or admissible hearsay
- Best evidence
- Not unduly prejudicial

There are significant barriers to undertaking the work on building a standardized methodology, and some of those are:

- Can be costly for all organisations to attain a standard and its relevant certification
- If a standard is voluntary it does not have to be followed and the industry remains in a flux position.
- Standards can be slow to evolve
- Standards can conflict globally
- Put restrictions on the innovative industries
- Can still be misinterpreted
- Can be cumbersome and increase time spent on a task
- Not enough support to implement them
- Difficult to understand, may be written in technical language
- Cannot confirm an expert's competence

## Feasibility

The aim of this research is to ensure that a global standard model for digital forensic investigations is feasible. A key is to understand the core reason for the requirement; this is the admissibility of digital evidence in a court of law. In their article Antwi-Boasiako and Venter [14] discuss the same issue of what test is applied to ensure that evidence is admissible, and they proposed a model for digital evidence admissibility assessment which has six characteristics:

- Typical legal requirements
- Legal Authorisation
- Digital Evidence Relevance
- Digital Evidence Authenticity
- Digital Evidence Integrity
- Digital Evidence Reliability

The six characteristics identified by the authors contain four key principles of Reliability, Relevance, Authenticity and Integrity and these are relevant for all evidence presented in a court. Reliability is in this instance concerned with being able to validate through repetition of tests so I have amended this to Repeatability. Therefore, these four elements will form the structure to determine the start point for the standardization of a model. As well as contemplating the admissibility of evidence, analysis of the legal requirements throughout the world will provide the foundations of what is acceptable in courts. This is essential because of the diversity of the legal systems and the jurisdictional boundaries that cause barriers to the common handling of cyber-crimes.

## Conclusion

In conclusion, this research has discussed the concept of a standard and an attempt has been made to develop a definition that can be used for the field of digital forensics. This has been developed as a foundation to discuss the feasibility of a standardized digital forensic investigation model. It has been possible to identify four key principles of admissibility which defines the output of the standardized digital forensic investigation, these four elements are repeatability, relevance, authenticity and integrity. Generating a global standard for digital forensic investigations using these four principles should be feasible if organizations work together. It is clear from the research viewed that there are a wide variety of digital forensic investigation models that have evolved over the last 20 years, there is a diversity in the models selected. Not all models have been selected by all authors for all comparisons, the reason for this is unknown, and possibly omitting them would better fit in with their proposed development.

There is one common outcome from all these comparisons, which is that it is essential to have a global standard method to allow digital evidence investigations to be considered scientifically sound. Although it is agreed that this is important and that there is a consensus on the need of a standard as well as the basic function of the standard, there is no focus from any formal group to expend the time to develop a standard.

## Recommendations for Future Research

If possible develop a consortium of global experts in the field of digital forensics and the legal profession as well as those from the

social sciences who can collaborate on building a new standard following the four principles and bringing together organizations that have already produced some very good research on what a new standard model should contain. A development of the research on barriers is recommended to enable these to be addressed by the consortium when developing a global standard. Continuing this research is important and the next stage should be to take the four principles of admissibility and identify those current models that contain these principles and creating the foundations for a common model. This research is a snapshot of the current position of digital forensics as a scientific field. It highlights the need for a standardized universal framework for digital forensic investigations and emphasizes the difficulties the scientific field could have in the future if no action is taken.

## References

1. Altoe R (2016) Digital Forensics in an eDiscovery World. Science Direct 6: 85-98.
2. Sammons J (2016) Digital Forensics Threatscape and Best Practices.
3. Crime Scene Forensics LLC (2018) History of Finerprints.
4. Reith M, Carr C, Gunsch G (2002) An examination of Digital Forensic Models. International Journal of Digital Evidence 3: 1-12.
5. Venema D (1999) Computer Forensics Analysis Class Handouts.
6. Prosise C, Mandia K (2001) Incident Response Investigating Computer Crime.
7. Sansurooa K (2006) Taxonomy of computer forensics methodologies and procedures for digital evidence seizure. Australian Digital Forensics Conference.
8. Yusoff Y, Ismail R, Hassan Z (2011) Common phases of computer forensics investigation models. International Journal of Computer Science and Information Technology 3: 17-31.
9. Valjarevic A, venter H (2012) Analyses of the state of the art digital forensic investigation process models. Institute of Electrical and Electronics Engineers. 74-83.
10. Casey E (2011) Digital evidence and computer crime forensic science, computers and the internet.
11. Jafari F, Shafique Satti R (2015) Comparitive Analysis of digital forensic models. Journal of Advances in Computer Networks 3: 82-86.
12. Takwa O, Belgacem C, Adel D (2016) A new digital investigation framework comparison method. International Journal of Computer Techniques. 3: 6-10.
13. Officers (2012) ACPO Good Practice Guide for Digital Evidence. London: ACPO.
14. Antwi Boasiako A, venter H (2017) A model for Digital Evidence Admissability assessment. Advances in Digital Foresics. 23-38.


Journal of Anesthesia & Clinical Care

Journal of Addiction & Addictive Disorders

Advances in Microbiology Research

Advances in Industrial Biotechnology

Journal of Agronomy & Agricultural Science

Journal of AIDS Clinical Research & STDs

Journal of Alcoholism, Drug Abuse & Substance Dependence

Journal of Allergy Disorders & Therapy

Journal of Alternative, Complementary & Integrative Medicine

Journal of Alzheimer's & Neurodegenerative Diseases

Journal of Angiology & Vascular Surgery

Journal of Animal Research & Veterinary Science

Archives of Zoological Studies

Archives of Urology

Journal of Atmospheric & Earth-Sciences

Journal of Aquaculture & Fisheries

Journal of Biotech Research & Biochemistry

Journal of Brain & Neuroscience Research

Journal of Cancer Biology & Treatment

Journal of Cardiology: Study & Research

Journal of Cell Biology & Cell Metabolism

Journal of Clinical Dermatology & Therapy

Journal of Clinical Immunology & Immunotherapy

Journal of Clinical Studies & Medical Case Reports

Journal of Community Medicine & Public Health Care

Current Trends: Medical & Biological Engineering

Journal of Cytology & Tissue Biology

Journal of Dentistry: Oral Health & Cosmesis

Journal of Diabetes & Metabolic Disorders

Journal of Dairy Research & Technology

Journal of Emergency Medicine Trauma & Surgical Care

Journal of Environmental Science: Current Research

Journal of Food Science & Nutrition

Journal of Forensic, Legal & Investigative Sciences

Journal of Gastroenterology & Hepatology Research

Journal of Gerontology & Geriatric Medicine

Journal of Genetics & Genomic Sciences

Journal of Hematology, Blood Transfusion & Disorders

Journal of Human Endocrinology

Journal of Hospice & Palliative Medical Care

Journal of Internal Medicine & Primary Healthcare

Journal of Infectious & Non Infectious Diseases

Journal of Light & Laser: Current Trends

Journal of Modern Chemical Sciences

Journal of Medicine: Study & Research

Journal of Nanotechnology: Nanomedicine & Nanobiotechnology

Journal of Neonatology & Clinical Pediatrics

Journal of Nephrology & Renal Therapy

Journal of Non Invasive Vascular Investigation

Journal of Nuclear Medicine, Radiology & Radiation Therapy

Journal of Obesity & Weight Loss

Journal of Orthopedic Research & Physiotherapy

Journal of Otolaryngology, Head & Neck Surgery

Journal of Protein Research & Bioinformatics

Journal of Pathology Clinical & Medical Research

Journal of Pharmacology, Pharmaceutics & Pharmacovigilance

Journal of Physical Medicine, Rehabilitation & Disabilities

Journal of Plant Science: Current Research

Journal of Psychiatry, Depression & Anxiety

Journal of Pulmonary Medicine & Respiratory Research

Journal of Practical & Professional Nursing

Journal of Reproductive Medicine, Gynaecology & Obstetrics

Journal of Stem Cells Research, Development & Therapy

Journal of Surgery: Current Trends & Innovations

Journal of Toxicology: Current Research

Journal of Translational Science and Research

Trends in Anatomy & Physiology

Journal of Vaccines Research & Vaccination

Journal of Virology & Antivirals

Archives of Surgery and Surgical Education

Sports Medicine and Injury Care Journal

International Journal of Case Reports and Therapeutic Studies

Submit Your Manuscript: http://www.heraldopenaccess.us/Online-Submission.php

Herald Scholarly Open Access, 2561 Cornelia Rd, #205, Herndon, VA 20171, USA.
Tel: +1-646-661-6626; E-mail: info@heraldsopenaccess.us
http://www.heraldopenaccess.us/