Reliability of Digital Evidence and Legal Matters: Ghana in Perspective

Michael Adjei Frempong
Accra, Ghana

Paul Asante Danquah, PhD
Accra, Ghana

ABSTRACT

The advent of technology has greatly affected how digital devices are used in recent days. The advancement in technology has enacted improved devices that evolve now and then with new features. These devices include a range of gadgets such as computers, mobile devices including phones, PDAs, digital cameras and calculators, ATMs, traffic lights, CCTV cameras, drones, body cams, and tracking devices. All of these have some form of memory that stores data which allows for the retrieval of digital evidence during digital forensic investigation for prosecution in a law court. Therefore, the methods used to acquire the evidence must conform to legal standards. For the digital evidence to be admissible, it must be reliable, and for reliability to be realized the evidence should be accurate, consistent, dependable, efficient, and relevant. The digital evidence collected must be so reliable to be admissible and devoid of legal challenges. This paper takes a look at Digital Forensics and some court cases concerning the reliability of the digital pieces of evidence collected and challenges with rules of evidence in Ghana. The paper further looks at Digital Evidence, sources and types, the laws governing the reliability of digital evidence, and the rules of evidence to its admissibility.

Keywords

Digital Forensics, Digital Evidence, Reliability, Rules of Evidence

1. INTRODUCTION

The advancement of Information Technology (IT) has catapulted an increase in the development of high-end digital devices including computers, mobile devices including phones, PDAs, digital cameras and calculators, ATMs, traffic lights, CCTV cameras, drones, body cams, and tracking devices. In Ghana, for instance, the law enforcement has installed at various sections along the roads and intersections in the cities ultra-modern closed-circuit televisions (CCTVs) that are been monitored from a central point in a bid to curb crimes. Individuals as well have also done the same in their various homes and offices. All of these devices have some form of memory that stores various data such as text, audio, still, and moving images captured on them. The high-level usage of digital-based devices has led to an increase in digital crimes paving the way for digital forensics investigation. This in turn has led to the generation of digital evidence on these devices. The increase in the production and complexity of digital evidence creation makes it difficult to reliably retrieve and collect evidence. The digital evidence must be collected in a conducive manner with less intrusiveness. Care must be taken by the investigator(s) such that the crime scene is properly secured and the evidence well preserved for collection. Law enforcement agencies use a variety of digital forensic methodologies during their investigations. This digital forensic investigation greatly relies on the digital evidence collected as it is the building block of the investigative process.

In Ghana, there are four (4) national agencies that are mandated with powers to investigate and prosecute matters concerning digital crimes. They are the Criminal Investigation Department (CID) of the Ghana Police Service, the Economic and Organized Crime Office (EOCO), the National Intelligence Bureau (NIB) formerly the Bureau of National Investigation (BNI), and the National Security Council Secretariat (NSCS). These institutions are charged with the requisite legal mandate and authority to investigate all offenses relating to digital and computer fraud.

The CID of the Ghana Police Service has six units including a Cybercrime unit responsible for forensic investigation including digital forensics. Below is statistical data obtained from the Ghana Police for Cyber Crime Reported cases between 2018 and 2020 [1].

Table 1:Cyber Crime Reported Case

Source: Ghana Police CID, SRMU, 2022.

CYBERCRIMES REPORTED AS OF OCTOBER 2021				
NO.	**CRIME**	**2018**	**2019**	**2020**
1	Obtaining Electronic Medium Payment Falsely	235	220	306
2	Personation	52	36	2
3	Stealing	64	62	55
4	Offensive Conduct	47	28	10
5	Unauthorized Interference with Electronic Record (ETA)	24	33	12
6	Charlatanic Advertisement	1	2	0
7	Publication of False News	23	15	6
8	Publication of Obscene Material	8	29	36
9	Threatening	19	17	39
10	Unauthorized Deposited Taking - Business (EBDSTI)	2	1	0
11	Extortion (COA)	5	52	167
12	General Provision for Cyber Offences (ETA)	3	14	6
13	Defrauding by False Pretense	13	54	149
14	Infringement of Copyright	1	1	1
15	Money Laundering	1	0	0
16	Kidnapping (COA)	4	0	3
17	Forgery of Document (COA)	2	2	1

18	Unauthorized Circumvention	5	7	0
19	Fraudulent Breach of Trust	3	2	2
20	Missing Person	2	0	0
21	Issue of False Cheque	1	1	1
22	The general offense for Fraudulent Electronic Fund Transfer	1	4	0
23	Attempt to commit a crime to wit obtaining electronic payment medium falsely	3	2	0
24	Illegal Device	1	0	0
25	Forgery of Trade Mark	1	0	0
26	Denial of Service	0	4	0
27	False Communication	0	0	0
28	Failure to Register	0	2	0
29	Child Pornography	0	0	0
30	Drug Trafficking	0	1	0
31	Abduction	0	1	0
32	Emotional Abuse	0	5	29
33	Illegal Possession of Exam Papers (WAEC)	0	1	0
34	Attempted Suicide	0	1	0
35	Preparation for Committing Certain Offence (COA)	0	1	0
36	Trading in Prostitution (COA)	0	1	0
37	Prohibition to purchase, obtain or Disclose Personal Data (DPA)	0	1	0
	Total	**521**	**600**	**825**

The table above indicates that there is a rise in reported cybercrime cases that calls for concern.

As a result of the vast use of digital devices digital data are most of the time all around and must be regularly acquired and collected in the investigation. Digital evidence can be used to reconstruct how a crime was committed that may provide investigative leads. It may also prove or disprove statements from witnesses which may lead to the likely suspects involved.

2. DIGITAL FORENSICS EVIDENCE

The proliferation of digital/cybercrimes has led to the rise of Digital Forensics(DF), one of the most important areas of a criminal investigation that aims at uncovering and examining evidence located at crime scenes. A definition by Palmer states that Digital Forensics is,

> *"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"*[2].

[3]also defined that not only looks at the process but also seeks legal prosecution.

> *Digital forensics combines computer science concepts, including computer architecture, operating systems, file systems, software engineering, and computer networking as well as legal procedures that describe criminal and civil litigation, cyber law, and rules of evidence.*

The goal of DF is to *identify digital evidence for an investigation* that uses both physical and digital evidence with scientific methods to conclude[4]. This then emphasizes that digital evidence must be preserved in all manner possible so that it can be admissible in the appropriate courts[5]. The result produced from Digital Forensic Investigation is Digital Evidence. The increasing use of digital evidence in legal prosecution offers a breakthrough in digital investigations and challenges as well. It was argued that the purpose of digital evidence is to provide consistent, relevant data that could be presented in a court of law or a public forum and it does not only fall under law enforcement.

[6]defines Digital evidence as "data or information of probative value stored on or transmitted by a digital device that supports or refutes a hypothesis formulated during a digital forensic investigation" relied upon in court to determine the outcome of a legal question.

Casey also states that Digital evidence is defined as any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred or that addresses critical elements of the offense such as intent or alibi[7].

[8]also gives a wider definition of DE as "information and data of investigative value that is stored on or transmitted by a computer". The wider nature of this definition is the use of 'investigative value', which is to mean all manner of investigations including data captured on physical objects.

In the legal circle, the Black Law Dictionary, 9th edition defines evidence as "something - including testimony, documents, and tangible objects - that tends to prove or disprove the existence of an alleged fact" or "the body of law regulating the admissibility of what is offered as proof into the record of a legal proceeding"[9].

This notwithstanding, legal interpretation of evidence differs in jurisdictions and Ghana is no exception. Ghana has enacted laws that deal with issues regarding digital evidence including the Criminal offenses Act, 1960 (Act 29), Evidence Act, 1975 (N.R.C.D, 323), Electronic Transaction Act, 2008 (Act 772), Electronic Communications Act, 2008 (Act 775), Economic and Organized Crime Office Act, 2010 (Act 804), Cyber Security Act, 2020 (Act 1038)[10].The Electronic Transactions Act, 2008 (Act 772) provide for the regulation of electronic records, making room for recognition of digital certificates, digital signatures, notarization, and automated transactions. This Act confers additional powers on Law enforcement agencies to arrest, search, and seize evidence. This act in a practical sense is subject to the Evidence Act.

The Evidence Act, 1975, (NRCD 323) sets out parameters to authenticate and identify electronic evidence. [11]categorizes evidence as:

1. Real Evidence: Evidence with characteristics that are directly and materially related to the case before the court. An example is a gun used by a suspect to commit murder.

2. Testimonial or Oral Evidence: Oral information is given in court, such as witness testimony.
3. Demonstrative Evidence: Information of an illustrative nature, such as pictures, site plans, and maps.
4. Documentary Evidence: Information in hard copies such as affidavits, business contracts, indentures, wills, etc.
5. Scientific Evidence: Technical or specialized information that is obtained through scientific methods.

From the categorization, [11] classifies digital evidence as scientific evidence and went on further that in the application of the law, digital evidence, though classified as scientific evidence may be considered hearsay evidence.

The Evidence Act, 1975 (NRCD 323) again gives the Court powers and the discretion on what evidence to admit. Core to the Evidence Act is RELEVANCE. Every evidence purported for tendering in court shall be relevant to the case at stake. This is referred to as the exclusionary rule where a judge has the discretion to exclude relevant evidence if the weight of considerations to the case is more the probative value of the evidence. This may be due to factors such as acquiring the evidence illegally, secretly, or the use of improper tools contrary to the rules of evidence.

Digital evidence has proven results in investigations. Despite the prevalence of digital evidence, few people are knowledgeable in the evidential, technical, and legal issues that relate to digital evidence and this has resulted in digital evidence often being overlooked, collected incorrectly, or analyzed ineffectively [12].

Digital evidence comes in various forms during criminal investigations which may include embezzlement, fraud, identity theft, homicides, sex offenses, child pornography and abuse, and drug peddling among others.

2.1 Sources and Types of Digital Evidence

Digital forensic evidence can be obtained from a variety of sources. Current digital devices have some digital computation and storage facilities exhibiting the input – processing – storage – output of the conventional computer systems such as laptops, desktop computers, PDAs, tablets, etc.

According to [13]sources of DE from these digital devices include Lost Data, Data Formats, and Data Storage media. Memory and Storage, Software, Processor. However, there are less obvious sources of digital evidence namely Gaming Systems, Video Cameras (Camcorders and CCTV), Removable Memory cards, Printers with internal hard drives, and Digital Picture frames.

From the sources of DE, some types of evidence that can be derived include Files, Deleted Files, Imaging, System and Program logs, Mobile Devices, Cache, and Temporary files.

2.2 Reliability of Digital Evidence

For the digital evidence to be appreciable in court it warrants that the evidence must be reliable. Reliability can be referred to as the process by which one obtains the same results by using an instrument to measure something (variables) more than once.

Basic reliability can be defined as the degree to which a research method produces stable and consistent results [14].

The reliability of digital evidence plays a critical role in the authentication process for admissibility.

From a legal standpoint, authentication is the process of determining whether the evidence is worthy. A quote by Reed, 1990 – 1991 states that Authentication means satisfying the court that

i. The contents of the record have remained unchanged.
ii. That the information in the record does originate from its purported source, whether human or machine.
iii. That extraneous information such as the apparent date of the record is accurate.

The core principle of Information Technology Security is based on three cardinal points: Confidentiality, Integrity, and Availability. By this guide, DF should also be guided by a core principle. The goal of the DF investigative process is to determine and link the extracted information i.e. DE to ascertain factual information for adjudication in court.

[15] opines that the fundamental principle of establishing factual information borders on three key variables: Reconnaissance, Reliability, and Relevancy.

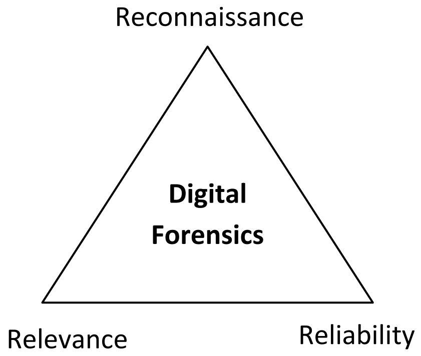

Fig.1 Adapted from Core Principle of Digital Forensic

Reconnaissance: The practice where a digital forensics investigator exhausts all possible methods, procedures, and forensic tools developed for a particular investigation type to collect, recover, decode, discover, extract, analyze, and convert data that is kept on diverse storage media to readable evidence irrespective of the source.

Reliability: The practice of maintaining the integrity of data without compromising the originality: collection, preservation, extraction, analyzing, and storing of data. This also ascertains that repeated test on the evidence will give the same result. Chain of custody should also be maintained in respect of time, the integrity of the evidence, and the personnel handling the evidence to ensure the reliability of the evidence.

Relevancy: This determines what evidence is to be collected during an investigation. Meaning evidence of prime importance to the case at hand, not just any evidence that does not relate to the case under investigation. Relevancy may be based on the weight and usefulness of the evidence.

The Electronic Transaction Act, Act 772 of Ghana provides four metrics for the admissibility of electronic evidence that state;

1. The reliability of how the electronic record was generated, displayed, stored, or communicated.
2. The reliability of how the integrity of the information was maintained.
3. How its originator was identified.
4. Any other facts that the Court may consider relevant.

The legal admissibility of electronic records in Ghana is faced with challenges such as functional policies and regulations, issues of authenticity, and issues of reliability, and accuracy.

Issues of reliability greatly rely on the tools and framework for the DF investigations. For example, if an unreliable tool that has not been forensically tested and accepted in the DF field is used or a tool is used wrongly at a phase where it ought not to be used may lead to an unreliable result hence unreliable DE that may lead to a conviction of an innocent person or free a suspect.

2.3 Rules of Evidence

The admissibility of digital evidence is a huge task in which Judges play a gatekeeper role to determine what scientific evidence is and is not admissible in their courtrooms [16]. In the USA for instance the courts are guided by Rule 702 of the Federal Rules of Evidence (FRE) regarding expert testimony which ensures that scientific testimony is both relevant and reliable for Judges.

Computer forensics and for that matter, digital forensics primarily is concerned with forensic procedures, rules of evidence, and legal processes, and the digital evidence must have all the attributes similar to that of traditional evidence presented in a court of law. The main concern therefore of digital forensics is accuracy and reliability.

The most commonly used standards are Frye, FRE 702, and Daubert standards. However, another standard is known as representational accuracy, which has gained tremendous support suggesting that one does not have to present all the originals. Bythis there exist a modern clause in the Federal Rules of Evidence (FRE 1001-3) which states, “If data are stored by computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original” [17].

The Frye Standard was derived from Frye v. the United States, 293 F.1013 (D.C. 1923) outlines that an opinion given by a forensic expert on scientific technique to the admissibility of digital evidence in court, such evidence will be accepted only where such a technique is accepted generally by the field’s scientific circles as reliable and relevant[18]. The Daubert Standard on the other hand was also born out of the Daubert v. Merrell Dow, 1993, which provides that a special pretrial be held to hear the scientific and digital evidence as well as procedures of discovery rules on the validity, reliability, benchmarking, algorithm and error rate are determined [19].

The Daubert Standard for admissibility establishes the requirement of relevancy and reliability[20].Researchers in time past have developed frameworks that tend to address the need to formalize the digital forensic process with most of them focusing on the collection and preservation of the evidence.

Ghana like any other country has come to accept the use of digital forensic evidence in the criminal justice system. The 1992 Constitution of the Republic of Ghana which is considered the supreme and the fundamental law provides law enforcement agencies in Ghana with the mandate to conduct criminal investigations. Article (19) of the constitution gives the power to law enforcement agencies for the management and disclosure of evidence during criminal proceedings in court. This means that the collection, preservation, and presentation of evidence, including digital evidence must be legal, and transparent in a manner that does not cause a miscarriage of justice [21].

As stated earlier all issues concerning electronic records in Ghana as captured in the Electronic Transaction Act 772 of 2008 which outlines the Admissibility of evidence which is subject to the relevancy section under the Evidence Decree Act of 1975 (NCRD 323).

Section 98 of the Electronic Transaction Act (Act 772) specifies what is known as “*Cyber Inspectors*” that mandates and empowers law enforcement officers to arrest offenders suspected to be cybercriminals. This section gives powers for search and seizure of evidence per the law. The Act makes it clear what and what not to seize during an investigation search. Section 98 clause 2 states that a “law enforcement officer may seize any computer, electronic record, program, information, document, or a thing in the execution of a warrant if the officer believes reasonably that an offense under the act is committed or may be committed”. The law specifies in sections 107-140 that all offenses are deemed and considered as cybercrime under Act 772.

The challenges of digital forensics can be categorized into three parts namely Legal, Resource, and Technical challenges.

The Legal challenges deal with privacy matters, jurisdictional issues, and the lack of standardized international legislation. The Budapest Convention on Cybercrimes for instance provides a mechanism for parties of the treaty to facilitate cross-border investigations and prosecutions but only 60 countries had acceded to this international treaty as of August 2018 [22]. Digital forensics practitioners and law enforcement agencies are faced with problems with respect to the passing of data protection and human rights laws regarding privacy. To ensure the integrity of digital evidence, the data should be collected and stored carefully and legally taking into consideration ethical matters. In the case of Raphael Cubagee vs Michael Yeboah Asare& 2 OrsSuit.No. J6/04/2017 for which judgment was passed on 28 February 2018 regarding the secret recording of conversations at the apex court of Ghana, the Supreme Court. In this matter, Plaintiff sought to tender in evidence in the form of a telephone conversation which was secretly recorded with a representative of the 3rd Defendant. In this case, the Judge stated, in terms of admissibility of evidence, that the secret recording of a telephone conversation was a breach of the privacy provisions of the 1992 Constitution under Article 18 (2). It was emphasized that the object of the constitutional rules on privacy was to protect “the individual against unwarranted intrusion, scrutiny, and publicity and guarantees his control over intrusions into his private sphere. Following are similar examples of legal challenges to evidence admissibility.

> *In the case between Edmund Addo VS the Republic of Ghana (Suit No. H/0080/2017), the applicant Mr. Edmund Addo was on May 27, 2016, for alleged defilement of a minor. The police subsequently affected Mr. Addo’s arrest and seized his electronic gadgets including a mobile phone, laptop, and an Internet modem. But those devices were secured with passwords which the applicant refused to give to the police when*

> *they (police) requested them. Upon refusal, the police engaged the service of an IT professional to break into the device for the police to collect evidence for prosecution. Mr. Addo through a Lawyer filed a case on June 13, 2016, against the IGP and Attorney General being the respondents, praying to the court that his right to privacy, property, fair trial, or education had been violated.*

The judgment, in this case, was given in favor of the applicant.

> *Again in the Civil Appeal judgment with suit No. H1/100/2017: EdemAdinyira (Plaintiff/Respondent) VS Scancom (1st Defendant/Appellant) and one other (2nd Defendant) given on July 27, 2017, held that the 1st Defendant violated the privacy of the Plaintiff by giving to the 2nd Defendant phone records of the Plaintiff without her knowledge, consent and authority and that it was wrongful, illegal and in contravention of the provisions of the Electronic Transactions Act, 2008 (Act 722) leading to the collapse of her marriage.*

The Appellate Court awarded damages in favour of Plaintiff.

Another is the ongoing trial case SUIT NO. CR/0401/2021, the Republic vs Dr. Frederick Mac-Palm and Others in which the trial judge gave a ruling as a result of objections raised by Defense Counsel, to the admissibility of audio and video recordings contained on a hard drive sought to be tendered in evidence by the prosecution. The defense counsel sought tochallenge the relevance and authenticity of the said evidence. The court ruled and I quote:

> "*Upon all considerations and the foregoing, as this Court has made a finding that all objections to the admissibility of the hard drive have no merit, same are for the avoidance of doubt overruled and dismissed in their entirety.*
>
> *This Court cannot conclude without stating that admissibility must be distinguished from weight or the probative value which the Court should attach to any evidence before it. The Defense is not precluded by this Ruling, from embarking on any exercise in that regard. The hard drive containing the audio and video recordings will be admitted in evidence and marked accordingly"*

The table below gives more examples.

Table 2: Court Cases with DE challenges. Source: Judicial Service of Ghana, 2022

Case	Status	Remarks/Issues
Rep. vs Dr. Mac Palm (2020)	Trial Ongoing	Audio and Video challenged for privacy, reliability, and authenticity.
Rep. vs Samuel Ofosu Ampofo& Kweku Buahen (2019)	Trial Ongoing	Audio evidence has been challenged for authenticity and reliability on the mode of acquisition.
Rep. vs Kwame Amponsah& 5 Other (2019)	Completed	Violation of Privacy
EdemAdinyira vs Scancom Ltd (2017)	Completed	Violation of Privacy, no warrant, or consent
Edmund Addo vs Rep. of Ghana (2017)	Completed	Violation of Privacy, Property, fair trial
Ackah vs ADB (2016)	Completed	Violation of Privacy
Rep. vs Alexander Tweneboah (2016)	Completed	Violation of Privacy
International Rom vs Vodafone Ghana (2016	Completed	Violation of Privacy
GFA vs EOCO	Completed	Violation of Privacy
Rep. Nana Ama Martins (2011)	Completed	Swap of an exhibit of cocaine (Breach of Chain of Custody)

It is clear from the above that admissibility of digital evidence in Ghana courts faces legal challenges due to non-adherence of rules of evidence. In most cases, court warrants were not obtained to access the digital evidence hence breaching the privacy of the party involved. A search and seizure warrant could be anticipatory, blanket, covert entry, and/or no-knock search warrants [23].

This study sought to look at some factors that determine the reliability of digital evidence in Ghana including Accuracy, Consistency, Dependability, Efficiency, and Relevance.

As stated by Hargreaves, in assessing the reliability of the source of information, several factors come to play including the authenticity of the information source, the accuracy with which the source captured the information, and the completeness of the information [24].

3. METHODOLOGY AND DATA ANALYSIS

The study used a mixed research methodology and questionnaire as the instrument. Data was collected using a primary source. All 50 participants were surveyed comprising judges and law enforcement agents.

3.1 Demographic Profile of Respondents

In total, 50 respondents participated in the study. 33 males and 17 females representing 66% and 34% respectively, with the majority falling in the age range of 51 – 60, 45 – 50, and below 45.

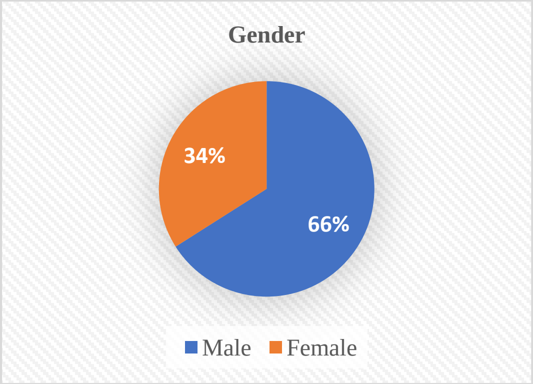

Chart 1 Gender Distribution

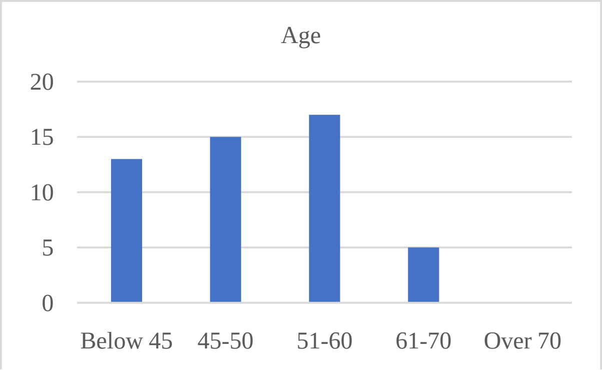

Chart 2 Age Distribution

3.2 Participants Education

A greater number of the respondents have acquired various academic and professional degrees. Most of the respondents have Bachelor’s degrees followed by Master’s Degree with fewer having Doctorate and Professional degrees.

Table 3: Participants Highest level of Education

Education	**Responses**
SHS	0
DIP/HND	0
Bachelor's Degree	21
Masters Degree	19
Doctorate Degree	3
Professional Degree	7

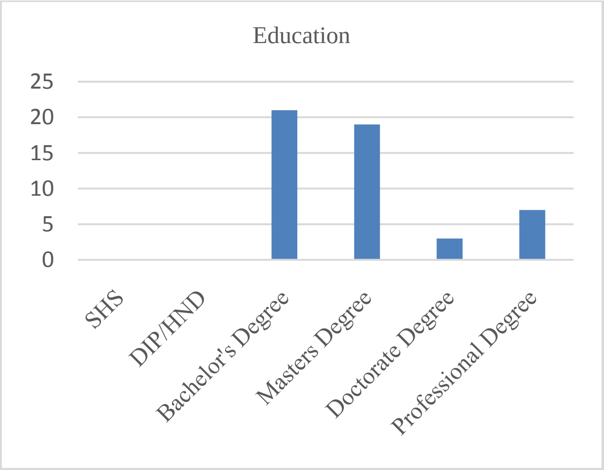

Chart 3 Highest Education Distribution

3.3 Work experience

However, many of the respondents have worked between 11 – 20 years representing 42 % followed by 34% for those who have worked less than 10 years.

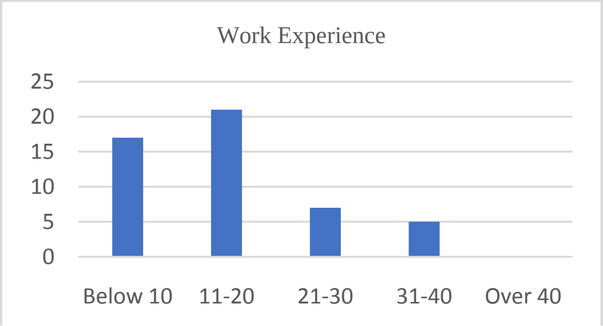

Chart 4 Work Experience distribution

3.4 Relevance as a determinant of reliability of DE and Ratings

The concentration of the study was to look at some factors that may determine the reliability of the digital evidence. The factors include Accuracy, Consistency, Dependability, Efficiency, and Relevance. All the respondents attested that all the factors specified are determining factors: Accuracy and Relevance scored 100% respectively. Consistency scored 92% with Dependability and Efficiency having 90% apiece as shown in table 4. Variance analysis was conducted for rating the factors on the bases of Very High to Very Low (1 - 5).

Table 4: Determinants of Reliability of DE

Determinants	Responses	%
Accuracy	50	100
Consistency	46	92
Dependability	45	90
Efficiency	45	90
Relevance	50	100

Table 5 shows the responses with regard to rating the factor which can determine the reliability of DE. Variance analysis was conducted for rating the factors on the bases of Very High to Very Low (1 - 5).

Table 5: Analysis of Ratings of factors determining Reliability of DE

SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
Column 1	5	168	33.6	26.8		
Column 2	5	40	8	31.5		
Column 3	5	19	3.8	1.2		
Column 4	5	11	2.2	1.7		
Column 5	5	12	2.4	1.8		
ANOVA						
Source of Variati	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*

on						
Between Groups	3590	4	897.5	71.23016	1.52E-11	2.866081
Within Groups	252	20	12.6			
Total	3842	24				

From table 5, above p-value of this analysis is p < 0.001 as indicated by p-value (1.52E - 11) and the test statistics F, reported in the analysis as 71.23 showing good significance concerning the response to the reliability factors. Computing the Cronbach's alpha gave α = 1 indicating a good reliability test. On the whole, the statistics from the respondents indicate that the fives factors determine the reliability of digital evidence.

Table 6: Ratings of Factors determining Reliability of DE

Task	Ratings				
	Very High	High	Mode rate	Low	Very Low
Accuracy	38	3	3	3	3
Consistency	28	14	5	0	3
Dependability	36	6	3	2	3
Efficiency	28	14	5	3	0
Relevance	38	3	3	3	3

3.5Accuracy

In determining the accuracy 35 participants representing 70% as against 30% require to see the original of the DE rather than a copy. Again 34 of the participants representing 68 % would require the type of DF tool used to acquire the DE to be presented as against 16 participants representing 32% as shown in table 7. Analysis from table 8,shows a p-value of 0.001 which indicates a statistically high significance of the task in the table. The analysis also from table 10, on the impact of extent of improper use of a tool, use of a wrong tool, and issues with chain of custody on the DE did show a p-value of 0.001, a highly significant statistically value in determining the accuracy of DE.

Table 7: Accuracy of DE

Task	Response		
	Yes	No	Total
Require Original evidence or Copy	35	15	50
Examiner/Prosecutor establishing type of tool used to acquire the DE	34	16	50

Table 8: Analysis of Accuracy of DE

SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
Column 1	2	69	34.5	0.5		
Column 2	2	31	15.5	0.5		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	361	1	361	722	0.001382	18.51282
Within Groups	1	2	0.5			
Total	362	3				

Table 9: Accuracy of DF tools

Task	Ratings					
	Very High	High	Mode rate	Low	Very Low	Total
To what extent would improper use of DF tool impact on the DE	18	26	6	0	0	50
To what extent will the use of the wrong DF tool impact the DE	18	20	9	3	0	50
Rate of issues regarding Chain of Custody of the DF investigation	37	13	0	0	0	50

Table 10: Analysis of the accuracy of DF tools usage

SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
Column 1	3	73	24.33333	120.3333		
Column 2	3	59	19.66667	42.33333		
Column 3	3	15	5	21		
Column 4	3	3	1	3		
Column 5	3	0	0	0		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Group	1514.667	4	378.6667	10.14286	0.001515	3.47805

s						
Within Groups	373.3333	10	37.33333			
Total	1888	14				

3.6 Efficiency as Factor determining Reliability of DE

Table 11 outlines tasks in terms of perceptions that seek to emphasize that efficiency can determine the reliability of DE. The table shows appreciable participants' views of the perception of investigators and prosecutors' ability to handle, understand and present DE in court. From table 12 it can be realized that Efficiency is statistically significant in determining how reliable a DE could be as indicated by the p – value of 0.006.

Table 11: Ratings of efficiency as a factor of Reliability of DE

	Ratings				
Task	Very Good	Good	Fair	Poor	Very Poor
Perception of the ability of investigators to identify, preserve, collect and examine DE reliably	6	15	20	6	3
Perception of the ability of prosecutors to effectively and reliably present DE in Court	6	15	26	3	0
How do the participants rate their perception to the understanding of DE	12	29	9	0	0

Table 12: Analysis of Perception ratings of Efficiency

SUMMARY						
Groups	*Count*	*Sum*	*Average*	*Variance*		
Column 1	3	24	8	12		
Column 2	3	59	19.66667	65.33333		
Column 3	3	55	18.33333	74.33333		
Column 4	3	9	3	9		
Column 5	3	3	1	3		
ANOVA						
Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	890.6667	4	222.6667	6.802444	0.006528	3.47805
Within Groups	327.3333	10	32.73333			
Total	1218	14				

4. DISCUSSION AND CONCLUSION

The main purpose of this study was to establish that Accuracy, Consistency, Dependability, Efficiency, and Relevance determines how reliable digital evidence can be in the Ghanaian perspective concerning legal rules of evidence. A review of some cases indicates that the core of admissibility as enshrined in Ghana's 1992 constitution and the Evidence Act 1975, (NRCD 323) emphasizes RELEVANCE which gives powers to the trial judge the discretion to admit into evidence, digital evidence. Forensic science that generated digital evidence is defined by the Black's Law Dictionary as "Evidence used in court especially evidence arrived at either by scientific means, by interpretation of patterns, or by a combination of experiential and scientific analysis" [25]. Scientific evidence on the other hand is given as "Facts or opinion evidence that purports to draw on specialized knowledge of science or rely on scientific principles for its evidentiary value as can be seen in the DAUBERT Test.Hence DE draws its strength from digitalization. The study, however, reveals from the respondents that all the five factors should be used concurrently to determine the reliability of the evidence as seen from the significance levels in the analysis tables. Interview conducted with some of the respondents reveals that Ghana's standards for conducting digital forensics investigations are by far below the international standards. The study reveals again that DE can be compromised to lose its reliability due to alteration to evidence during collection, examination, and analysis. Inappropriate use of a tool, outdated tools, and no adherence to chain custody may also impact the reliability of the DE. And that the law enforcement agents must follow basic principles of the rules of evidence to make the digital evidence very reliable for trial. That DE has come to stay as a result of the current technological advance of most crimes committed wholly or partially through electronic mediums. Moreover,trainingneeds to be conducted on this topic for police investigators, lawyers, judges, prosecutors,etc to enable the courts and the justice system to appreciate how important DE is to the resolution of cases, be it civil or criminal. It is the anticipation of the study that the legal fraternity will take into cognizance the factors determining the reliability of digital evidence, work towards the acceptance of legal standards within law enforcement agencies and apply them. It is the hope that this study will open further studies in the field of digital evidence concerning knowledge and presentation of digital evidence by Court Prosecutors which will go a long way to contribute to the body of knowledge.

5. REFERENCES

[1] Ghana Police, (2022). Cyber Crimes Report (2018-2020). SRMU.

[2] Palmer, G. (2001). A Road Map for Digital Forensics Research. Utica, New York.

[3] Kerr, O. S. (2009). Computer crime law (2nd ed.). St. Paul. : MN: Thomson/West.

[4] Hewling, Sant. (2012). Digital Forensics: An Integrated approach, Proceedings from 6th Cybercrime Forensics Education and Training. Canterbury, UK: Canterbury Christchurch University, Canterbury, UK

[5] Carrier, B. (2003). Defining Digital Forensic Investigation. International Journal of Digital Evidence.

[6] SWGDE, (2011), Digital & Multimedia EvidenceGlossary Version: .4

[7] Casey, E. (2011). Digital Evidence and Computer Crime. 3rd Edition. San Diego, California. USA: Elsevier Inc.

[8] ACPO, (2007) Good Practice Guide for Computer-Based Electronic Evidence, Version 3

[9] Adjei, D. D. (2018). Criminal Procedure and Practice in Ghana. Accra: G - PAK Ltd.

[10] Republic of Ghana, Acts of Parliament

[11] Brobbey, S. A., (2014), Essentials of the Ghana law of evidence, Accra, Ghana :Datro Publications.

[12] Mason, S., Weir, G.R.S. (2017). The Sources of Electronic Evidence. London: University of London Press: Institute of Advanced Legal Studies.

[13] Dudovshiy, J. (2018). The Ultimate Guide to Writing a Dissertation in Business Studies: Step-by-Step Assistance. Research Methodology.net.

[14] Ieong, R. (2006). FORZA, Digital Forensics Investigation Framework that incorporates legal issues. Proceedings of 6th Annual DFRWS, (pp. 29-36).

[15] Cohen, F. B. (2015). Digital Diplomatics and forensics: Going forward on a Global Basis. Records Management Journal, 25(1).

[16] Vacca, J. R. (2005). Computer Forensics: Computer Crime Scene Investigation. 2nd Edition. Boston, Massachusetts: Charles River Media, Inc.

[17] Nagy, Palmer, Sundaramurthy, Campbell. (2017). An empirical study on Current Models for reasoning about Digital Evidence. Proceedings of 10th Intl. Conference on Systematic Approaches to Digital Forensic Engineering.

[18] Apau, Richard; Koranteng, Felix. (2020). An Overview of the Digital Forensic Investigation Infrastructure of Ghana. Forensic Science International: Synergy, 299 – 309.

[19] Antwi-Boasiako, A. (2018). A Model for Digital Evidence Admissibility Assessment (Doctorial Dissertation). Pretoria.

[20] Hargreaves, C. (2009). Ph.D. Thesis: Assessing the Reliability of Digital Evidence from Live Investigation involving Encryption. Cranfield University.

[21] Black’s Law Dictionary, 9th Edition, 2009, Thomson Reuters, USA