Awareness and Understanding of Computer Forensics in the Ghana Legal System

Michael Adjei Frempong
Research Scholar
Sikkim Manipal University
Accra, Ghana

Kamal Kant Hiran
Head, Department of IT
Sikkim Manipal University
Accra, Ghana

ABSTRACT

In this era of Technological age also called digital age, most transactions are conducted electronically. This modern-day paradigm makes way for the possibility of harmful unanticipated information security breaches of both civil and criminal nature. However, there is a tremendous knowledge gap in the legal system concerning computer/digital forensics with respect to digital evidence. Courtroom and Legal issues relevant to computer/digital forensics are extensive and differs with respect to procedural evidence rules that ensure reliability of the evidence so produced in the court of law for fair adjudication. Electronic evidence is very fundamental to the successful handling of cases related to such information security breaches.

This paper on the impact of awareness and understanding of computer/digital forensics in the Ghana Legal System especially Judges, with regards to the electronic evidence, laws and jurisprudence covered twenty (20) superior Judges. The findings revealed a gap between the Judges and issues on computer forensics which if not looked at may create problems in relation to the influx of computer related crimes.

General Terms

Information Security, Computer Forensics, Legal System

Keywords

Computer Forensic, Digital Evidence, Admissibility, Rules of Evidence.

1. INTRODUCTION

The world today has and continues to witness the advancement of information technology which provides limitless benefit for individuals, businesses, commerce and industry. Unfortunately this same media is used by unscrupulous persons for acts of criminality.

In recent times there has been increase in computer related crimes including hacking, forgery, fraud, illegally spreading pornographic materials, sabotage, copyright infringement, etc. As early as 2002 the FBI stated that fifty percent of the cases reported are computer crimes [1].

According to Internet Crime Complainant Center (IC3) 2012 report, the organization received 289, 874 complaints with an adjusted dollar loss of $525, 441, 110 representing an increase of 8.3% since 2011 reported losses [2].

Technologies of today such as cellular phones, Pagers, iPods, Internet, and websites have added another dimension to crime. For example, in the past property crime perpetrated by criminals involved face – to – face interaction with the victim. But today the criminals sit in the comfort of their homes to commit property crimes using computing devices.

The computer and law enforcement professions are faced by these challenges and have to develop expertise to combat these crimes by the use of collection and analysis of digital evidence [3].

The Computer Forensics domain is vast and broad. To this end, this research will be focusing on the Impact of Awareness and Understanding of Computer/Digital Forensic by Judges and Counsels in respect to admissibility of digital evidence in court will explore the legal aspects of computer forensics and how it may be contested in the court system.

Ghana Legal System

Ghana legal system recognizes both common law and customary law. The Constitution is the highest law of the land and there are provisions for legislation by parliament and other institutions. The common law system is adversarial in that the opponents are given the opportunity to present their cases to an independent judge who delivers a judgment after hearing the parties. Customary law is generally relevant in matters dealing with land tenure, law of succession and family law.

The Ghanaian Judiciary consists of the Superior Courts of Judicature, which include the Supreme Court, the Court of Appeal, the High Court, Regional Tribunal and the lower courts currently comprising the Circuit Courts, the District Courts.

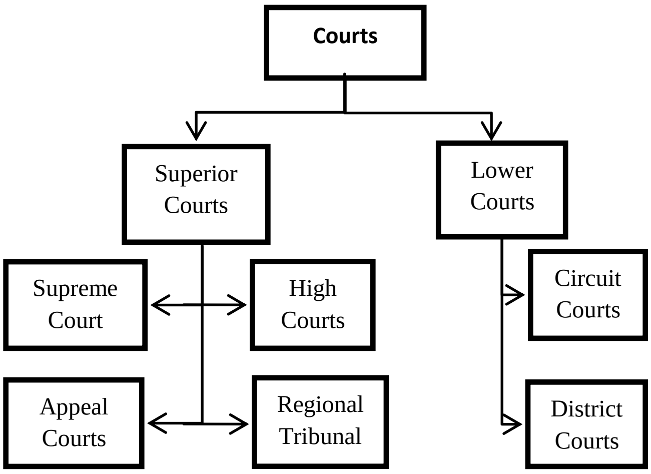

Fig 1: The Court Structure

The High Court has divisions aimed at promoting specialization. They are;

- The Fast Track Courts
- Commercial Courts
- Human Rights Court
- Economic and Financial crimes Courts
- Industrial and Labour Court
- Land Courts
- Family Court
- Probate and Administration

With the increase in computer related crimes the courts are presented with all kinds of evidences that need to be well understood by the Judges, counsels and prosecutors alike for fair delivery of justice.

The Judicial Service since 2001 has embark on ICT training for all Judges to be able to understand some basic computing concept as well as generating judgments on their own. However, there still lies a problem when it comes to digital forensics as this area seems to be a specialized area.

2. DEFINING COMPUTER FORENSICS

Computer Forensics is about evidence from computers that is sufficiently reliable to stand up in court and be convincing. Computer forensics, also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence [4].

Computer Forensics which is a sub – discipline of Digital Forensics emerged as a response to the escalating rate of computer related crimes. Computer can be used as either an instrument to commit crime, an object of crime, or a repository of evidence.

Among the various definitions given to Computer Forensics by various researchers including the following;

- Computer Forensics is simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence [5].
- Computer Forensics is using an expert to preserve, analyze and produce data from volatile and non – volatile media storage [6].
- Computer Forensics is the collection, preservation, analysis, and presentation of computer-related evidence [7].

2.1 Computer Forensic

The product of Computer Forensics is Digital Evidence which can also be referred to as Digital Forensic Evidence [8].

Judges to some extent have minimal knowledge and understanding the nature of digital evidence and using it applicably to which more has to be done as the credibility of the justice system is at stake.

According to Casey Judges, Counsels and Jurors must be knowledgeable in a variety of areas in ICT so as to make informed and concise decisions on the admissibility of digital evidence [9].

According to Mason (2008) there are complex situation resulting from the difficulties encountered by individuals to their applying of critical analysis with regards to statements offered as facts in the courtroom based on computer/digital forensic evidence [10]. For example,

- A Judge may be presented with network server/event viewer logs showing an intrusion in an organization’s system by a cyber-intruder using a particular Internet Protocol (IP) address. However, Internet service provider (ISP) records show that the IP address used by the intruder was assigned to a computer in a particular residence at the time of the incident. This information could be misleading and be used to improperly identify an individual as the offender.

- A Judge is presented with call history and service provider records showing that one mobile telephone was used to place a call to another mobile phone. The court and a jury might erroneously believe that this evidence conclusively proves that the owners of the two telephones actually had a conversation when the phone could have been stolen to place the call.

- When Microsoft office suite is installed metadata, which is data about data, include the name of the person who registered the product. This name will appear in every document generated by the Office application. A Judge might mistakenly rule that the metadata in a given document convincingly attests that the named person is the actual person who generated the document.

2.2 Rules of Evidence

The admissibility of digital evidence is a huge task to which Judges play a gatekeeper role to determine what scientific evidence is and is not admissible in their courtrooms [11]. 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 on Judges.

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

Evidence is that which is offered before a court of law to persuade it to reach a particular view of events which may be in dispute and could be Direct, Real, Documentary, Demonstrative/Testimonial, Technical, Expert or Derived evidence.

Typically there are five basic rules to the collection of electronic evidence. The evidence must be Admissible, Authentic, Complete, Reliable, and Believable.

Vacca in his book Computer Forensics: Computer Crime Scene Investigation, 2nd edition, the entire scientific evidence standards are [12].

- Relevance test (FRE 401, 402, 403)
- Frye standard (Frye v. U.S., 1923)
- Coppolino standard (Coppolino v. State, 1968)
- Marx standard (People v. Marx, 1975)
- Daubert standard (Daubert v. Merrell Dow, 1993)

Unlike the Frye standard which outlines that an opinion given by a forensic expert on scientific technique to the admissibility of digital evidence in court will be accepted only where such a technique is accepted generally by the field’s scientific circles as reliable and relevant and the Daubert standard which also provides that a special pretrial be held to hear the scientific and digital evidence as well as procedures of discovery rules on validity, reliability, bench marking, algorithm and error rate are determined which are used in the USA, the admissibility of evidence in courts of Ghana is by the Evidence Decree of 1975 (NCRD 323) containing eleven parts.

2.3 Uses of Computer Forensics

Computer forensics is mostly and has been and continues to be used in various fields including civil and criminal litigations, research in academia, educational studies, corporate world etc.

Computer forensics in the corporate world is used for civil litigations. Researches in academia delve into the improvement of the emerging field. This is then taught to educate on the computer forensic field. Last not the least is the use of computer forensic by the government including the law enforcement agencies.

3. RELEVANCE AND SIGNIFICANCE

Judges as gatekeepers determines what evidence will or will not be admissible in their courts. This therefore goes to say that the admissibility of digital evidence from computer forensic investigation for a trial is based upon the decision of the trial Judge [13].

By Ball Judges must determine the acceptability of scientific and technicalities of computer forensics testified by an expert witness [14]. Judges compared to attorneys have less experience when it comes to computer forensics. This is because prosecutors and attorneys gets to see digital forensic evidence more often thereby have more familiarity with it [15].

Marsico just like Van Buskik and Liu in their seminar papers observed that with respect to Daubert standard's reliability, veracity and reliability, even when digital evidence is introduced by an expert's testimony especially in criminal trials attorneys infrequently raise a challenge [16].

Legal issues pertaining to computer forensics includes

- Acceptability
- Admissibility of evidence
- Analysis and Preservation

Where evidences are not challenged by defense attorneys, Judges are left little opportunity to make informed decision about admissibility or authentication of digital evidence [17].

With the widespread usage of computers, electronic mail (e – mail), mobile devices as well as web service, Judges with more insight on ICT are more willing to accept digital evidence than their colleagues with little knowledge. It is established that Judges in larger courts especially those in the cities who are exposed to more technology have greater familiarity with ICT and tend to accept digital evidence compared to their peers in remote areas.

Computer forensics places much importance and accuracy to the results it so produces – digital evidence – and by this Judges attaches high level of credibility to the evidence. This may be as a result of the Judge's lack of and understanding of how the evidence was derived to which the evidence may have been altered, manipulated and may be misrepresented. It is then suggested that the Judge's familiarity and comfort with ICT have influence to the admissibility of evidence in their courts.

The awareness and understanding of the Judge's knowledge in computer forensics is very important to the making of conscious decisions about the acceptance and admissibility of digital evidence in terms of veracity, reliability and accuracy.

Thus it is established that Judges are not very knowledgeable on matters of computer forensics than the contestants of the judicial system and that Judges need to educate themselves on topics relating to cases in their courts.

The goal of this study then is to determine and create a framework that will enable Judges to have the appropriate skills and knowledge in computer forensics necessary for accepting, understanding and interpreting digital forensic evidence.

For instance in the case of "The Republic vs. Mathias Bill (alias Delali Vettel, alias Robert Scott)" pending in one of the High. Mathias, twenty – one years old has been arrested and charged of defrauding by false pretence, a complainant Kathleen D. Mincz of U.S.A through electronic transaction as well as money laundering. The fact of the case is that Mathias, a Ghanaian, pretended to be an American by name Robert Scott to defraud the complainant to some huge amount of US dollars

Now counsel for the accused raised a preliminary objection to the use of video link (video conference) at the instance of Attorney General's Department and Economic and Organized Crime Office for the witness (complainant) to testify to the court citing Part Three of the Criminal Procedure Code, 1960 (Act 30). The objection was dismissed. The counsel not satisfied has filed a motion for interpretation at the Supreme Court.

The onus is now on the Judge to be able to understand forensic aspect of the case and this brings to fore-light the understanding and handling of digital evidence. Hearing continues.

Second example, the case of the Republic vs Kwabena Amaning alias Tagor and Alhaji Issah Abass. The two persons were convicted to fifteen (15) years in prison on charges of conspiracy to commit crime namely Prohibited Business relating to Narcotics. They were arrest upon a group conversation which was recorded by an unknown person. The content was said to have contain some elements bordering on narcotics and the reproduction of the said conversation made on compact disc (CD) used as evidence. They were subsequently jailed in 2007.

The defense counsel filed an appeal on the grounds that the CD presented as evidence,

1. Violated the constitutional rights to their freedom from the interception of the private conversation without due process of law; and
2. The origin and authenticity of the CD do not measure up to the required legal standards as set out in the Evidence Decree of 1975, NCRD 323.

The defense counsel also made reference to Article 18(2) of the 1999 Constitution.

Subsequently the accused persons were in 2009 acquitted and discharged.

4. RESEARCH METHODOLOGY

4.1 Research Design

Research design as defined by Parahoo is a plan that describes how, when and where data are to be collected and analyzed.

Grounded Theory (GT) is the research methodology employed for this study. GT, introduced in 1967 by Glaser and Strauss in their book "To Generate or Discover a Theory", is one of the ever improving qualitative research strategies.

Grounded Theory can be defined as the discovery of theory from data systematically obtained from social research.

Grounded theory is a methodology intended for developing inductive theories that are grounded in steadily gathered and analyzed data. Data collection, analysis, interpretation, and theory development are done iteratively and interdependently.

4.2 Proposed Variables

Specifically, twenty (20) superior Judges of Judicial Service HQ including Supreme Court, Appeal Court and High court used for the study. However random sampling will be used in selecting the sample size for the administration of the questionnaires.

4.3 Research Instrument for Data Collection

The study used closed – ended and open – ended questionnaire as well as interviews to collect data. The researcher further reviewed secondary data and published text as well. The data was analyzed qualitatively in an attempt to compare the findings from the primary data with the meanings derived from the secondary text for the purpose of using it to find the knowledge gap of computer forensic awareness to Judges.

5. PRESENTATION OF RESULTS

The survey touch on several questions including personal demography, computer forensic and digital evidence, IT and Internet applications just to mention a few. Of interest to this paper are responses to computer forensic and evidence, familiarity ratings and forensic evidence standards. The following extracts from the study.

Computer Forensic definition:

All the respondents except two representing 10% accepted the definition. The two were of the view that computer forensic is not yet popular in the Ghanaian Judicial System which might be evolving. So no clear definition to their understanding can be preferred.

Familiarity Rating:

Respondents answered questions to their familiarity with Digital Evidence (DE), Computer Forensic Process (CFP), Computer Technology (CT) and Internet Applications (IA) on the scale of one (1) being low, two (2) below average, three (3) Average, four (4) above Average and five (5) also being High. See table 1.

Table 1. Respondents Familiarity with IT, Computer Forensics, etc.

RESPONDENTS	DE	CFP	CT	IA
R1	2	1	3	-
R2	2	2	2	2
R3	3	1	2	2
R4	4	2	3	3
R5	2	3	3	2
R6	1	1	1	1
R7	3	3	3	3
R8	1	1	1	2
R9	4	3	1	2
R10	3	3	3	5
R11	3	2	3	3
R12	5	3	3	4
R13	3	2	3	3
R14	4	-	3	5
R15	2	3	4	1
R16	3	2	2	2
R17	4	4	3	4
R18	3	3	3	4
R19	3	2	2	1
R20	4	2	1	2

Table 2 shows the number of respondents to each of the rating metrics percentage wise.

Table 1. Percentage of Ratings

RATING	DE	%	CFP	%	CT	%	IA	%
LOW	2	10	4	20	4	20	3	15
<AVG	4	20	7	35	4	20	7	35
AVG	8	40	7	35	11	55	4	20
>AVG	5	25	1	5	1	5	3	15
HIGH	1	5	0	0	0		2	10
NOT SURE	0	0	1	5	0		1	5
TOTAL	20	100	20	100	20	100	20	100

From table 2 it realized that only one respondent, representing 5% scored high, 2 respondents representing 10% scoring low and 8 respondents representing 40% on the average with respect to Digital Evidence (DE). For CFP 4 and 7 respondents representing 20 and 35 percent respectively rating for low, below average and average as well with none scoring high. However, 1 respondent was not sure of familiarity with CFP. In the case of CT 11 respondents representing 55% scored average. In the area of IA only 2 respondents representing 10% were much familiar with Internet Applications with 1 not sure of familiarity.
On factors that influenced the ratings, it could be deduced from table 3 that 1 respondent was influenced by all factors including specifying international conferences as the other option. 10 were influenced by only Personal Experience, and 1 by Education only. See table 3.

Table 2. Rating Influence Factor

RESPON DENTS	EDUC ATION	PERSO-NAL EXP.	PROFES-SIONAL EXP.	OTHE R
R1	0	1	1	0
R2	0	1	0	0

R3	0	1	0	0
R4	0	1	0	0
R5	0	1	1	0
R6	0	1	0	0
R7	1	0	1	0
R8	0	1	0	0
R9	1	0	0	0
R10	0	1	1	0
R11	1	1	1	1
R12	1	1	0	0
R13	0	1	0	0
R14	0	1	1	0
R15	0	1	0	0
R16	0	1	0	0
R17	1	0	1	0
R18	1	1	1	0
R19	0	1	0	0
R20	0	1	0	0
TOTAL	6	17	8	1

NOTE: O = Not selected 1 = Selected

Forensic Standards and Rules of Evidence:

Unlike the USA and elsewhere standards such as the Frye and Daubert standard are applied to computer forensic cases, the Ghanaian Judicial System does not have a particular standard to follow. The Ghanaian Judicial System only relies on the Evidence Decree of 1975 (NCRD 323), the High Court Rules and the Criminal Procedure (Act 30). It established that where a defense council does not raise questions and objections on acceptance of the evidence because none familiarity with processes in computer forensics the Judge is left with little to do in terms of accepting digital evidence.

On the issue of what is considered to the admissibility of digital evidence, 12 (60%) respondents chose relevance of evidence only while 8 (40%) respondents chose both relevance of evidence and reliability of evidence with none choosing reliability only.

On issues faced to deciding on challenges to accepting digital evidence it was a break-even of 10 respondents choosing a Yes and a No respectively? However, one respondent who answered to a Yes did indicated that relevancy and credibility where the main issues and that new rules are being considered by the General Legal Council to amend the Constitutional Instrument (C.I) 47.

Few of the Judges interviewed did indicate that they neither had taught programs on ICT at the undergraduate level nor at the professional level which makes them somewhat vulnerable to ICT related programs. It is either through their own personal experience, training at the Judicial Training Institute and/or international conferences that sort of enlighten them on ICT.

6. CONCLUSION

The results above clearly indicate that there is a bit of knowledge gap with regards to understanding of computer forensic by Judges. Though Judges do not need to be experts in computer forensic and IT, it is important that they have some general knowledge to understand this field better.

The data so collected provided enough insight to make recommendations with regards to training format and pattern that will build the needed trust by the Judges on matters of computer forensics.

In general, all the Judges contend that they need to know more so as to better understand issues on computer related crimes that will in-turn have greater impact of fairness and just on same.

7. RECOMMENDATION

The purpose of this paper was to find out the impact of awareness and understanding of computer forensic by Judges. From the data collected it is recommended that;

1. Judges need to read more literature on matters concerning computer forensic as the rate at which computer related crime are perpetrated are on the ascendency.

2. The Judicial Training Institute should organize regular training sessions on this topic for the Judges.

However, it is very important that the laws schools incorporate some ICT related programs into their curriculum.

8. ACKNOWLEDGEMENT

We would like to express our gratitude to our Dean Dr. Abhishek Tyagi and Director Academics Mr. Gajendra Singh for their guidance and contributions. We would also like to thank our family members for their support.

9. REFERENCES

[1] Reyes, A & Wiles, J., 2007. The Best Damn Cybercrime and Forensics. Burlington: MA. Syngress Publishing Inc.

[2] IC3, 2012. 2012_ic3report.pdf. Retrieved November 18,2013, from http://www.ic3.gov/media/annualreport/

[3] Vacca, J. R., 2005. Computer Forensics: Computer Crime Scene Investigation, 2nd Edition. Boston, Massachussetts: Rinvers Media Inc.

[4] Robbins, J., An Explanation of Computer Forensics, PC Software Forensics.

[5] Mack, M. 2003. Electronic Discovery Versus Computer Forensics. Law Journal1, New Jersey.

[6] Cohen, F. 2008/2010. Challenges to Digital Forensics Evidence/Digital Forensics Examination, 2nd Edition. Livemore, CA: ASP Press.

[7] Casey, E., 2011. Digital Evidence and Computer Crime: Forensics Science, Computer and the Internet, 3rd ed. Amsterdam, Netherlands: Elsevier Academic Press.

[8] Mason, S., 2008. Judges and Technical Evdience, 2nd International Conference on Cyberforensics Education and Training. Canterbury, UK.

[9] Cohen, F. 2008. Challenges to Digital Forensics Evidence. Livemore, CA: ASP Press. Kerr, O. S., 2009. Computer Crime Law, 2nd ed. St. Paul. MN: Thomson/West.

[10] Wegman, J., 2005. Computer Forensics: Admissibility of Evidence in Criminal cases. Journal of Legal Ethical and Regulatory Issues 8(1).

[11] Ball, C., 2008. What Judges should know about Computer Forensics. National Workshop for District Judges II.

[12] Rogers, M., Scarborough, K., & San Martin, C., 2007. Survey of Law Enforcement perceptions regarding Digital Evidence. In P. Craiger & S. Shenoi, eds., International Federation for Information Processing (IFIP). Boston, MA: Blackwell.

[13] Marisco, C., 2004. Computer Evidence V. Daubert: The coming Conflict (CERIAS Tech Report 2005-17). Retrieved November 19, 2013, from htt://www.Cerias.purdue.edu/booksshelf/archive/2005-17.pdf.

[14] Van Buskik, E., & Liu, V.T., 2006. Digital Eivdence: Challenging the prersumption of reliability. Journal of Digital Forensic Practice 1(1), 19 – 26.

[15] Losavio, M., Wilson, D., & Elmaghraby, A., 2006. Prevalence, Use and Evidentiary issues of Digital Evidence of cellular telephone consumer and small – scale digital devices. Journal of Digital Forensic Practice, 1(4), 291 – 296.

[16] Parahoo, K., 1997. Nursing Research: Principles, Process, Issues. London: Macmillan.

[17] Glaser, B.G., & Strauss, A.L., 1967. The Discovery of Grounded Theory: Strategies for Qualitative Research. New York: Aldine de Gruyter.