Components of Sound Forensically Acquisition of Digital Data

[1] Joyce Chepkemoi Chepkwony; [2] Masese B Nelson

[1, 2] School of Science Engineering and Technology
Department of Computer science & Information Technology
Kabarak University, Private Bag 20157, Kabarak, Kenya

Abstract - As the attacks on the cyber space continue to intensify, digital crimes continue to be reported at large. The current techniques used by forensic investigators through the incident response operations include mostly pulling out the power cable of the suspected machines. This method normally causes major interference of the evidence gathering process, hence the need to examine the essential components that makes up forensically sound digital data acquisition process. Descriptive research design was adopted and use of questionnaires in collecting data. 89.4% respondents established that there was need for additional, review and improvement of the tools regularly. The study recommends investigating agencies to channel more resources towards digital evidence acquisition tools to improve effectiveness of digital evidence. The study portrayed that the institutions lacked well-established digital forensic labs with modern equipment and that a small percentage (19.1%) only do validate the tools to operate as intended.

Keywords - *Cyber crime, Digital, Evidence, Forensic, Investigation.*

1. Introduction

In recent years, it has come to a realization that only trying to prevent information technology incidents is insufficient, as literature shows that a determined attacker with sufficient resources will finally succeed in breaking or avoiding the measures taken. As such, organizations are taking a more holistic approach to information security, detective, implementing preventive and taking responsive measures (Fielder *et al.,* 2016). Kshetri (2013) points out that with the current future, the value of forensic computing will increase for the Kenyan companies, to the law enforcers and to the legal practitioners. There are fundamental reasons that demand more concentration and attention to the cybercrime and the capacity to support in investigation and prosecution of cyber offenders.

Digital crime encompasses not only new crimes but also those that have been in existence committed using digital techniques. The boundaries of forensic science are expanding, and so is the need for trained professionals. The centre of excellence in digital forensics provides a mechanism to meet these challenges. Security agencies typically use either Encase or Forensic Toolkit to do their forensic evaluation of the client's hard drives (Taylor *et al.,* 2014). The established forensic tools, during investigations are limited by their inability to preserve the hardware and software state. Investigators do shut down the machine so as to inspect the contents of the disk and identify the artefact of interest. This process breaks the network connections and also unmounts encrypted disks in computers causing significant loss of evidence and possibility of disruption of critical systems (Taveras, 2013).

1.1 Statement of the problem

Computer technology is the major important part of daily human life and growing rapidly fast. This growth comes with the increase of computer crimes such as unlawful intrusion, financial fraud, identity and intellectual theft. To counteract these computer-related crimes essential components in digital forensic evidence need to be identified. Computer forensics involves acquiring and analysing digital information for use as evidence in criminal, civil or administrative cases (Soltani & Seno, 2017).

The growing incidence and risk of inappropriate, illegal or criminal computer behaviours has increased the need to build bridges between technical and legal areas of expertise in order to produce more effective defensive and offensive responses (Hannan *et al.,* 2003). The acceptance and development of digital forensics in Kenya has been very slow because of the inappropriate regulatory policies, standards, procedures, technologies, and legal and governance challenges. For the progress of computer forensics, the law ought to keep pace with the advancement of the technology mostly in components in use.

1.2 Objective of the Study

To examine the essential components that makes up forensically sound digital data acquisition process.

2. Literature Review

2.1 Components for Forensically Sound Digital Data Acquisition

Overill & Chow (2018) argues that, for evidence to be forensically sound, the disk image must be an exact copy of the original one. The disk image process must include a means for verifying the authenticity and also the reliability of the copying process. Adams (2013) notes that, unlike some other areas that carry out forensic practice, digital forensic practitioners do work in a number of different environments and the existing methods tend to focus only on particular areas such as law enforcement, thereby failing to put into account the other needs of the other fields working in other areas like the incidence response.

2.2 Computer Forensic

Computer forensics is a branch of digital forensics that use analysis techniques to gather potential evidence from desktops, laptops and server computers for investigating suspected illegal or unauthorized activities. More precisely, computer forensics focused on finding potential digital evidence after a computer security incident has occurred (Crouch, 2012). Computer Forensics is an emerging field and there is less standardization and consistency across the courts and industry (Walsh, 2018). Each of the computer forensic methods is focused on particular areas such as electronic evidence discovery or law enforcement. There has never been a single digital forensic investigation technique that has been accepted universally. However, it was generally accepted that the digital forensic technique must be flexible, in that it can support any type of incidents and the new technologies (Adam, 2013).

Digital forensics is a branch of forensic science often related to computer crime, and includes investigation and recovery of materials which are found in digital devices (Pichan, Lazarescu, & Soh, 2015). Casey (2011) says digital forensics deals with the application of scientific knowledge for collecting, analyzing, and presenting legal evidence. Digital evidence, in its nature is extremely fragile therefore; it can be easily altered, damaged or even destroyed by inappropriate handling or examination. For these reasons high precautions ought to be taken to safeguard this type of evidence. Failure to do so could render it unusable or lead to an inaccurate conclusion. Training or studies on technology acceptance by the law enforcers may lead to effective use of digital forensics (Lin, Hu, & Chen, 2004).

2.3 Technologies Used in Forensic

Technologies such as Digital Surveillance for Xbox (XFT) device is useful as the XFT sessions can later be replayed during court hearings in real time. This toolkit allowed law enforcement agencies to scour the inbuilt hard disk of such devices and find illicit hidden materials easily (Xynos *et al.,* 2010). It was developed to allow authorities visual access to hidden files on the Xbox hard drive. Kaur, Saini and Sood (2013) states that the investigators used a Video Spectral Comparator 2000 device to look at pieces of paper in case there were any hidden or obscured writing, that one could determine the quality of the paper and analysis done even if the paper was damaged by fire or water. According to Garfinkel and Simson (2010), digital forensics tools have not kept up with cyber crime and the technology since the current digital forensics tools were designed to help investigators find specific evidence and not to assist in investigations.

2.4 Investigators

The investigators argues that, in exceptional situations where a person sees a necessity in accessing original data which is held on a storage media or a computer, that person or the forensic practitioner should be proficient in doing so and able to prove the relevance and the outcome of their act (Eales, 2016).

There are four principles as per the investigators which should be adhered to. These are; ***Principle 1:*** The data stored in the computer should not be altered or changed, as they can be later presented in the court; ***Principle 2:*** The Person handling the original computer data should be competent enough, and shall also be able to give the evidence explaining the relevance and course of their actions; ***Principle 3:*** The documentations and audit trail for the procedures applied to computer-based electronic evidence should be created and preserved in that any other person should be able to scrutinize those processes and attain same result; ***Principle 4:*** The person who is responsible for the investigation will have an overall responsibility for accounting that the law and the ACPO principles are adhered to.

2.5 Tools and Materials for Collecting Digital Evidence

There are tools for processing computer crimes. Following is table 1 showing a summary of the functions of the tools.

Table 1: Comparison of Forensic Tools Function

Function	**ProDiscover Basic**	**OSForensics, demo version**	**Access Data FTK**	**Guidance Software EnCase**
Acquisition				
Physical data copy	√	√	√	√
Logical data copy	√	√	√	
Data acquisition formats	√	√	√	√
Command-line processes				√
GUI processes	√	√	√	√
Remote acquisition		√	√	√
Validation and verification				
Hashing	√	√	√	√
Verification	√	√	√	√
Filtering		√	√	√
Analyzing file headers		√	√	√
Extraction				
Data viewing	√	√	√	√
Keyword searching	√	√	√	√
Decompressing			√	√
Carving		√	√	√
Decrypting		√	√	
Bookmarking	√	√	√	√
Reconstruction				
Disk-to-disk copy	√	√	√	√
Partition-to-partition copy	√	√	√	√
Image-to-disk copy	√	√	√	√
Image-to-partition copy	√	√	√	√
Disk-to-image copy	√	√	√	√
Rebuilding files	√	√	√	√
Reporting				
Bookmarking / tagging	√	√	√	√
Log reports		√	√	√
Report generator	√	√	√	
Automation and other features				
Scripting language				√
Mount virtual machines		√	√	√
E-discovery		√	√	√

(Source: Nelson, Phillips & Steuart, 2014)

Table 1 shows a list of some of the computer forensic tools and their functions. A tick (□) mark represents where a particular function is available in the tool. As observed, the computer forensic tools are unable to present an impression for all the data found on a media device. To find the right forensic tool function to use depends on the type of case the forensic investigator is currently working on.

Table 2 shows a summary of the division of tools either static or live.

Table 2: Exploring Static and Live Digital Forensics: Methods, Practices and Tools

Sr. No	Tool Name	Op Sys	Purpose/Description	Static/ Live Analysis
1.	Registry Recon	Windows	This tool is used to rebuild the registries of Windows from any place of a hard drive and further it is parsed for the analysis in depth.	Static
2.	SIFT (SANS Investigative Forensics Toolkit)	Ubuntu	SIFT is used to perform digital forensic analysis on different operating system.	Live
3.	EnCase	Windows	This tool is used to gather and analyze memory dump in digital forensic investigation in static mode	Static
4.	Digital Forensics Framework	Windows/ Linux/ Mac OS	During the live and static analysis, DFF is utilized as a development platform and digital investigation tool.	Both
5.	EPRB (Elcom soft Password Recovery Bundle)	Windows	This toolkit is used to perform digital analysis on encrypted system, password recovery and data decryption.	Live
6.	PTK Forensics (Programmers Toolkit)	LAMP	It is GUI based framework for static and live analysis.	Both
7.	FTK (Forensic Toolkit)	Windows	This tool is used to perform digital analysis and indexing the evidentiary data.	Static
8.	The Coroner's Toolkit	Unix	It is a command line user interface tool to perform forensic analysis on Unix systems.	Both
9.	The Sleuth Kit	Unix/ Windows	Toolkit provides GUI and command line interface to per-form digital forensic analysis in Unix and windows.	Live
10.	COFEE (Computer online forensic evidence extractor)	Windows	COFEE is used to extract and analyze forensic data lively.	Live
11.	OCFA (Open Computer Forensics Architecture)	Linux	It is a command line interface for distributed	Live

			computer forensics and it is used to analyze digital media. It is mostly used in digital forensic labs.	
12.	OS Forensics	Windows	This tool is used to perform analysis on E-mail, Files, Images and web browsers.	Live
14.	Safe Back	Windows	This tool is used for evidence collection, analysis and for creating backup of evidentiary data in digital media.	Static
15.	Forensic Assistant	Windows	It is used to analyze the activities performed by user on internet like emails, docs and IM and web browsers.	Live
16.	X-Way Forensics	Windows	This tool is used for the general purpose on Win Hex editor used to perform static and live analysis.	Both
17.	CAINE (Computer Aided investigative environment)	Linux	Command line user interface used for distributed and standalone computer forensics.	Both
18.	bulk extractor	Windows, Linux	For the extraction of phone numbers, email addresses, URLs and the other objects which are identified.	Live
19.	IRCR (Incident Response Collection Report)	Windows	Collects live forensics information from the command history, computer, network connection, current processes, opened ports, registry start up information and event logs from system.	Live
20.	Intella	Windows	It is used to process and investigate Email, digital data and Cell phones.	Live
21.	CMAT(Compile Memory Analysis Tool)	Windows	It extracts information from the memory dump and also exposes malware.	Live
22.	WFT (Window Forensic Toolkit)	Windows	Toolkit used to analyze the memory, system information, file/directory timestamp, port number, user information,	Live

(Source: Rafique, & Khan, 2013).

Table 2 shows that forensic analysis can be done either in static or live modes. It is evident by the above table that traditional approach provides incomplete evidentiary data compared to live analysis tools which provide the investigators with more accurate and consistent picture of current and previous running processes. This implies that live analysis is more reliable in forensic data.

2.6 Digital Forensics security fundamentals

According to Thomas (2018), evaluation of forensic evidence actually should be scientific, including that the reliability of methodologies be testable, and requiring that forensic evidence be evaluated and presented to the courts in a logically correct manner.

2.7 Chain of Custody

Chain of custody is the procedure that an item of evidence be proved to be genuine to the level its proponent claims it to be. According to Cosic and Baca (2010), chain of custody is the chronological documentation or paper trail, showing the paper trail, custody, control, transfer, analysis, and disposition of physical or electronic evidence. This starts exactly from the moment of entry of crime scene till the end of the court case. Giova G. (2011) also gives another definition as the procedure for handling evidence in a series of investigations. That is a procedure for performing documentation to the evidence in chronological events. Documenting each and every change in the evidence and assessing in perspective of the final analytical results (Casey, 2007). This is the basic part of the validity of the case and the forensic soundness of the evidence. According to Dykstra and Sherman (2012), chain of custody is authentication or identification of real evidence (that is; tangible evidence that is historically connected with a criminal case and not merely illustrative).

3. Methodology

The study employed a descriptive research design. A purposive sampling technique was used in the study in selecting of the sample. Purposive sampling aims at a particular group and a sample is not produced that is a representative of a larger population, though it can be closely what is required (Etikan *et al.,* (2016). The sampling size used based on the above purposive sampling was 52 respondents.

3.1 Instrumentation

The questionnaires were used by the researcher to collect data. They were constructed based on the research objective. The researcher preferred the questionnaires since they were easy to administer and time saving. The questionnaire contained closed-ended questions using liker scale (ranging from 1= No Extent; 2= Little Extent; 3= Moderate Extent; 4= Large Extent; 5=Very Large Extent). There were also a few open-ended questions which brought forth qualitative data on subjective thoughts and different responses related to access to digital evidence acquisition tools.

4. Data Analysis

Descriptive analysis was done using the Statistical Package for Social Sciences (SPSS). Quantitative research method was used which is evident by the questionnaires.

4.1 Components for Forensic Digital Evidence.

Table 3: Components for Forensic Digital Evidence

Statement	SD	D	N	A	SA
I feel that there is need for other additional digital forensic tools to the institution	0.0%	6.4%	4.3%	12.8%	76.6%
We use tools that are thoroughly tested and acceptable legally	0.0%	0.0%	29.8%	53.2%	17.0%
I think digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions	25.5%	36.2%	19.1%	19.1%	0.0%
We have a well-established digital forensic lab with modem equipment/tools	14.9%	70.2%	2.1%	12.8%	0.0%
The institution ensures the tools they use to acquire digital evidence are validated to operate as intended and accurately acquire data	8.5%	53.2%	19.1%	19.1%	0.0%

**Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree,
A = Agree**

It was established that 89.4% declared that there was need for additional digital forensic tools to the institution. It was also affirmed by 70.2% respondents that they used tools that were thoroughly tested and acceptable legally. It was noted that 61.7% of respondents disagree that digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions as they lacked a well-established digital forensic lab with modern equipment and tools (85.1%). Only 19.1% agreed that the institution ensured that the tools they used to acquire digital evidence were validated to operate as intended and accurately acquired data. According to the study, it is very important for any criminal investigator, to have in mind that use of tools and technical skills alone is not enough to fully investigate any digital crime but also handling, storage and validation of the tools used in acquiring digital evidence should be adhered to.

5. Conclusion

The study aimed at investigating the essential components of digital forensics evidence in organisations that use digital forensic evidence. That would assist in achieving high digital security level parameters and shortening the analysis time of computer forensic investigations. ICT is dynamic and new issues keep emerging. In lieu of this, digital forensic evidence acquisition and handling tools and components need to be reviewed and improved regularly. Digital forensic technique must be generally flexible, in that it can support any type of incidents and the new technologies.

5.1 Areas of Further Improvement

The study is not limited to only these organisations but open to all forensic investigative institutions. The production of computers and mobile phones in our societies is at its rise. The worldwide mobile phone subscriber base has reached around 4.4 billion. Almost two thirds of the worldwide population currently use mobile phones (Zhang *et al.,* 2015). Mobile applications would also be ideal in this case because of the fast emerging mobile technologies and ease of use.

References

[1] Adams, Richard (2013). *"The emergence of cloud storage and the need for a new digital forensic process model"* (PDF). Murdoch University.

[2] Casey, E. (2007). *What does "forensically sound" really mean? Digital Investigation.*

[3] Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press

[4] Ćosić, J., & Bača, M. (2010). A framework to (im)prove chain of custody in digital investigation process. In *Proceedings of the 21st Central European Conference on Information and Intelligent Systems (CECIIS)* (pp. 43-438).

[5] Crouch, J. E. (2012). *An introduction to computer forensics*. NSCI; http://www.nsci-va.org/WhitePapers/2010-12-16-Computer% 20Forensics-Crouch-final.pdf.

[6] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*, S90-S98.

[7] Eales, N. (2016). Risk assessment. *Missing Persons: A Handbook of Research*, 160.

[8] Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4.

[9] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13-23.

[10] G. Giova, (2011)., "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *Int. J. Comput. Sci. Netw. Secur.*, vol. 11, no. 1, pp. 1–9, 2011.

[11] Garfinkel, Simson L. (2010). Digital Forensics Research: *The Next 10 years.*

[12] Hannan, T. H., & McDowell, J. M. (2003). The determinants of technology adoption: The case of the banking firm. *The RAND Journal of Economics*, 328-335.

[13] Kaur, R., Saini, K., & Sood, N. C. (2013). Application of video spectral comparator (absorption spectra) for establishing the chronological order of intersecting printed strokes and writing pen strokes. *Science & Justice*, *53*(2), 212-219.

[14] Kshetri, N. (2013). *Cybercrime and cyber security in the global south*. Springer.

[15] Lin, C., Hu, P. J., and Chen, H. (2004). Technology implementation management in law enforcement: COPLINK system usability and user acceptance evaluations. *Social Science Computer Review*, 22(1), 24-36.

[16] Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations*. Cengage Learning.

[17] Overill, R., & Chow, K. P. (2018). Measuring Evidential Weight in Digital Forensic Investigations. In *IFIP International Conference on Digital Forensics* (pp. 3-10). Springer, Cham.

[18] Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, *13*, 38-57.

[19] Rafique, M., & Khan, M. N. A. (2013). Exploring static and live digital forensics: Methods, practices and tools.

International Journal of Scientific & Engineering Research, *4*(10), 1048-1056.

[20] Soltani, S., & Seno, S. A. H. (2017). A survey on digital evidence collection and analysis. In *Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on* (pp. 247-253). IEEE.

[21] Taveras, P. (2013). SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific Journal, ESJ*, *9*(21).

[22] Taveras, P. (2013). SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific Journal, ESJ*, *9*(21).

[23] Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism.* Prentice Hall Press.

[24] Terrizzano, I. G., Schwarz, P. M., Roth, M., & Colino, J. E. (2015, January). Data Wrangling: The Challenging Yourney from the Wild to the Lake. In *CIDR*.

[25] Thomas, J. E. (2018). *Using Digital Forensic Techniques to Investigate and Detect Ransomware Infection*.

[26] Walsh, S. J. (2018). Australasian forensic science summit 2016: the external future context and the case for change. *Australian Journal of Forensic Sciences*, *50*(3), 245-258.

[27] Xynos, K., Harries, S., Sutherland, I., Davies, G., & Blyth, A. (2010). Xbox 360: A digital forensic investigation of the hard disk drive. *Digital Investigation*, *6*(3-4), 104-111.

[28] Zhang, Y., Wu, J., Zukerman, M., & Yung, E. K. N. (2015). Energy-efficient base-stations sleep-mode techniques in green cellular networks: A survey. *IEEE communications surveys & tutorials*, *17*(2), 803-826.

Additional information:

Joyce Chepkemoi Chepkwony is currently a PhD student at Kabarak University, Kenya. She holds a Master of Science degree in Information Technology Security & Audit from Kabarak University, Nakuru, Kenya. Her research interests mainly include digital forensics and network security.