IJEMD-CSAI, 1 (1) (2022), 41 – 49 https://doi.org/ 10.54938/ijemdcsai.2022.01.1.37

International Journal of Emerging Multidiciplinaries:
Computer Science & Artificial Intelligence

Research Paper
Journal Homepage: www.ijemd.com
ISSN (print): 2791-0164

IJEMD International Journal of Emerging Multidisciplinaries
COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE

Cyber Crime and Digital Forensics: A Pragmatic Framework for Sudanese Courts

Saad Subair[1*], Derar Yosif[2], Abdelgader Ahmed[3], and Christopher Thron[4]

[1]University of Africa, [2]Sudan Judge Authority, [3]Legal Firm, Free Lance, [4]Texas A&M university
**Corresponding author*

Abstract

Cyber crime is becoming more frequent in our daily life since computers are everywhere now and hence the term cyberspace is becoming our ordinary life. Digital forensics or computer forensics which the process of securing digital evidence against the crime is becoming inevitable. Digital evidence is the foundation for any digital forensic investigation that can be collected by several means using technologies and scientific crime scene investigation. Modifications with crime scene data may possibly change the evidences that may lead to different investigation results. Several models and frameworks to help investigating cybercrimes have been proposed. In this paper we are proposing a frame work that to suit the Sudanese judiciary system. The framework suggested studied several models and frameworks in the globe to come out with a suitable framework model that can help the Sudanese courts taking their decisions concerning cybercrime. The conventional chain of custody is our main platform to construct our framework. That is due to fact that computer crime is different from conventional crime in that it may have no definite place or space. Although The share of people in computer crime is more crucial than the technology itself, achieving evidence integrity is more challenging than normal crimes. This work aims to study and evaluate the applicability of existing digital forensic process models to the Sudanese environment, analyze each of these frameworks might and then construct a framework to Sudan courts.

Keywords: Digital Forensics Framework; Digital Forensics; Chain of Custody; Cyber Crime; Computer Crime; Cyberspace.

1. Introduction

Computers have become the norm of today’s atmosphere and we use them in almost every aspect of our ordinary life. They are everywhere, from shopping, banking, schools, roads, sports, and pockets. Modern life depends on these computers devices and the internet to do their daily transactions, marketing and communications across the world. Big volume of information that includes financial and personal information is stored on these computer systems.. The term Cyberspace which describes the space of cyber or in technical terms, a notional environment of computers and computer networks over which communication and interaction take place appeared in the computer world in the eighties [1,2 ,3].

Email addresses: ssubair@gmail.com (S. Subair)

Cyberspace has become the space of millions of people who use it every day to share their ideas and thoughts, play games, communicate through social networks, buy and sell through business and commerce cyber hubs. Cyberspace has also gained its own value, which can be seen in the form of various applications and services people use in their everyday lives. Cyber space now is considered a real world [4].

Cyberspace has no physical barriers and hence, is not restricted by any territorial limits. Today, any computer connected to the internet in any part of the world can share information with any other computer in anywhere in the world without considerable barriers and limitations. The only condition that you are not part of cyberspace is to isolate your computer or your organization from connecting to the internet.

Everyone can get free knowledge and information from the materials available over the cyberspace. The advent of online education platforms have enabled people to access knowledge which was earlier restricted in schools. As far as the the E-government is concerned, cyberspace made all transactions and form submissions easy job. Processing national ids driving license, telephone bill and electronic payments can be done over cyberspace while people sitting in their homes or offices. Just like any normal activities in life where it involves many people with different backgrounds. attitudes, and intends, cyberspace cannot be considered fully trustworthy, many people suffer from the crimes over the internet which is known as cybercrimes. With the increase in the scope of computer networks, the world has seen a rise in computer crimes that is more than have of the people surveyed assured the increase of these computer crime. [1,2,3,4].

2. Review

In fact cybercrimes came to existence with the existence of computers. The main issue in cybercrime is that the suspect or the criminal can stay undisclosed in crime scene or sphere **[1].** Cyber crimes may occur when a person target a computer or a system with the aim of corrupting, illegally extracting the data, deleting the stored data, or even just seeing it. Many people, from computer experts to the legal firms describe or define the term cybercrime, the legal firms define cyber crimes as a crime or any illegal activity that involves a network and a with a device or a computer. **[1,3]** . As mentioned earlier, one fact remains the same that cybercrime unlike traditional crimes, provides a major barrier in unveiling the criminals as the user’s identity may be hidden or fraud over the virtual domain or the cyberspace. Cybercrimes cause damages to people in their personal, business, formal, and social lives. Authorities estimate cybercrime damages in billions of dollars and this damage may be discovered after several years.[1,3,5]. There are many types of cybercrimes reported around the world, these crimes differ in nature due to what is known as "Modus Operandi" which is defined as the way criminals commit their crimes. Table 1 shows the different types of cybercrimes with their explanations and some known cases of them.

Table 1: Types of Cybercrime, their Explanations, and some known cases

Type Of Cybercrime	Explanation	Known Case
Unauthorized Access	Accessing data or information that one is not authorized to see or access	From students in universities to professional hackers, it is the naive computer crime.
Identity Theft	A person pretending or acting to be someone else.	Facebook, Tweeter and many social networks suffers from identity theft
Denial Of Service DoS	Overloading a computer system by sending too many requests at once which result in failure to complete normal requests.	Big businesses suffer from DoS. Usually hackers ask for money or ransom.
Phishing	Attracting individuals or luring them into giving up their personal or financial	LinkedIn website was cloned in order to steal the credentials of the users.

	information then abusing them. In a different way, some hackers call this Social Engineering	
Fraud	Shaping or Manipulating financial data of someone else in order to benefit from it. It is a kind of deception.	Employees of a bank in India that made a link with Citibank of New York were arrested for alleged fraud of thousands of dollars
Cyber Terrorism	The terrorist groups use the internet and social media as a platform to spread terrorism agenda and anti-government philosophy.	Christchurch terrorist used the internet to send a message to the PM office and then used Facebook to broadcast a life of his crime.
Intellectual Property Theft	It can be defined as the stealing of any property or material that is copyrighted. .	Yahoo filed a case in India court against Akash Arora for using ‘yahooindia.com’ as a domain name which resembles the website ‘yahoo.com’
Spoofing	A person takes up other person’s identity in order to penetrate in the system or to shift the blame onto that person . Scam can be near to this**.**	An Indian executive pretended as a girl and cheated an UAE man through the internet.
Malwares	Like viruses, worms, Trojans and spywares. They capture critical information like, id, passwords, username, keystrokes.. etc	The internet is full with malicious programs or malwares
Spamming	Distributing unwanted e-mails to various email addresses. Many might be automatically generated	Everyone in the internet suffers from these Spasms. Businesses are worst suffering.

Therefore, as the extent of damage increases the need of an investigation process investigator become essential. The Oxford dictionary broadly defines the word forensic as “relating to or denoting the application of scientific methods to the investigation of crime” , also it defines it as relating to courts of law”. The forensic sciences along with logical reasoning can be considered as the primary foundation for solving cybercrime cases. As forensic science proved to be successful in solving a number of traditional cases it can also be used in the crimes of computers or cybercrimes. This method which uses the systemic analysis and investigations is known as digital forensics, some people also refer to as computer forensics [1,2,3,4,5]. This emphasizes the fact that forensic activity usually relates to courts of law. It is important that, forensic investigation is conducted in a scientific way and with a legal bases.

Digital forensics can also be defined as “analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media or data which is stored or encoded for finding evidences” [4].

Once these basics are in place, the next step is to apply a sound forensic framework, which will consistently gather evidence suitable for presentation in a court of law, to ensure that criminal behavior can be successfully prosecuted [1,4]. A digital forensic framework can be defined as a chart or a flow structured to lead to a successful forensic investigation. This implies that the conclusion reached by one digital forensic expert should be the same as any other person who has conducted the same investigation or framework [4]. A forensic investigation has to be conducted in a scientific manner and must comply with all legal requirements. Evidence shall be collected in the manner described in the framework specified [1,3].

A suggestion or documented case alone will not lead to a complete solution of a problem or a cybercrime. A framework depends on a number of flow structures or other sub frameworks that are based on a given logic. Digital forensics framework depends on laws and legislation as much [8]. There are many of forensics models that have been proposed shows the complexity of the digital forensic process. Most focus on the investigation, Another framework is proposed which focuses on processing and examining digital evidence. The phases of this model are: recognition; preservation; classification, and reconstruction [2]. This model also concentrates into the investigation domain of the forensic process.

In 2004 **An Extended Model of Cybercrime Investigations** is proposed. The phases or activities of the model are: awareness; authorization; planning; notification; search for and identify evidence; collection; transportation; storage; examination; hypothesis; presentation; proof/defense, and dissemination [9]. This may be considered as the more comprehensive model at that time. Table 2 shows different digital forensics tools or packages that are frequently employed in forensic investigations with their explanation and use [17,18].

Table 2: Some Famous Digital Forensic Investigation Tools or programs

Tool	**Explanation**	**Use**
osquery	osquery is a constant monitor of the system state and does not target the restoration of deleted files.	Can detect Retefe Banking Trojan by continuous monitoring
FTK Imager	FTK Imager is a data preview and imaging tool that allows to examine files and folders on hard drives, network drives, CDs/DVDs, and review the content of forensic images or memories.	SHA1 or MD5 hashes of files can be created. Then export files and folders from forensic images to disk. You can also view files in Windows Explorer
LastActivityView	Allow to view what actions were taken by a user and what events occurred on the machine Activities like running an executable file, opening a file/folder, an application or system crash or a user performing a software installation will be registered in a log file.	The information can be exported to a CSV / XML / HTML file. This tool is useful when you need to prove that a user performed an action he denied.
GRR	The main benefit of GRR is its capability to check actual file content and search for strings that can be attributed to known malware It allows looking for changed files in the overall OS structure.	GRR Rapid Response is an incident response framework focused on remote live forensics.GRR consists of two parts: client and server. It works just like osquery
Paladin Forensic Suite	Paladin Forensic Suite is a Live CD based on Ubuntu	There are over 80 tools on this CD dealing with Imaging,

	that is packed with many open source forensic tools.	Malware Analysis, Social Media Analysis, Hashing, etc.
USB Historian	It parses USB information, from the Windows registry, to give a list of all USB drives that were plugged into the machine. It displays information such as the name of the USB drive, the serial number, when it was mounted and by which user.	These information can be very useful when you need to understand whether the data was removed, moved, or accessed
Autopsy **(Sleuth Kit)**	It is a digital forensics platform with a GUI that is used to understand what happened on a computer.	It comes with features like Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching It can recover deleted files from unallocated space.
CAINE **(Computer Aided Investigative Environment)**	It is a Linux Live CD. Features include a GUI, semi-automated report creation and tools for Mobile Forensics, Network Forensics, and Data Recovery	CAINE environment is designed to assist investigators in all four stages of an investigation: preservation, collection, examination, and analysis
COFEE **(Computer Online Forensic Evidence Extractor)**	It MS toolkit acts as an automated forensic tool during a live analysis. It contains features and a GUI that guides you through data collection and examination and helps generate reports after extraction..	It is a forensic toolkit used to extract evidence from MS Windows computers
Wireshark	It is used by governments and big corporate across the world. It enables looking at a network at the microscopic level. then admin can scan for malicious activity.	It is the world's most-used network protocol analysis tool. It may be used with Xplico tool. You can extract e-mails.

The Liforac Model [13] is a live forensic acquisition processing model that collects the evidence from live acquisition to counter the problems caused by dead acquisitions them into a legally framework. The developed model in [14] followed basic concept of Liforac Model [13], but unlike the Liforac Model's technical key pillars they adopted key principles Reconnaissance, Relevancy and Reliability but the working sense is similar. The model also paid full attention on flow of process according with the judiciary norms which also been done in Liforac Model [13]. The Hybrid Model of Magkos [15] adopted the same guidelines that mentioned in the two previous models that concentrated on filling the gap in-between physical and digital evidence. Cosic and Cosic[16] used the chain of custody platform to develop their model. their work presented a basic concept of chain of custody of digital evidence" and "life cycle of digital evidence". It addressed an additional phase in the life cycle in digital archiving. Again like the previous models this model has limitation in other phases.

Lim and Lee[12] used what is called the XeBag concept to solve the problem of digital chain of custody The solution is a combination of using of PKZIP compression data format with metadata representation through the XML format.

3. METHODOLOGY

There are many models and frameworks suggested by many researchers to deal with the cybercrimes and digital forensics. As mentioned previously, cybercrimes are known by their nature that evidence are not physically identified or known. Digital evidence need special way to deal with. It is quite difficult to file a complete chain of custody when dealing with the digital evidence[10]. Below we show the processes of two models and then in the next section we are suggesting our model to Sudanese courts

In step-wise the extended model of Ciardhuain [9], involves the following digital forensics processes and phases: It includes 13 steps to solidify a cybercrime digital evidence and then present it to the court.

1. Awareness
2. Authorisation
3. Planning
4. Notification
5. Search for and identify evidence
6. Collection of evidence
7. Transport of evidence
8. Storage of evidence
9. Examination of evidence
10. Hypothesis
11. Presentation of hypothesis
12. Proof/Defence of hypothesis
13. Dissemination of information

We also consider the steps or procedures of digital forensics process of Harbawi and Varol [4]. The researchers here put in consideration the ubiquity of the cyberspace where individuals, states, organizations share the same space or the same techniques. The steps or the areas are:

1. Identification
2. Acquisition
3. Preservation
4. Examination/analysis
5. Presentation

We studied several models and frameworks as can be seen in the above review of literature, however, two models are presented here as examples only since almost all the models or frameworks share the same phases or activity processes. We will use these frameworks as a methodology to construct our model.

4. RESULTS AND DISCUSSION

Since the overall goal is to produce concrete evidence suitable for presentation in a court of law, maybe the best way to get the benefit from all models is to study them together and see how your environment suits each model or you may construct a hybrid model. We build our model based on the following observations: the mentioned model are builds on the knowledge domain of the previous ones; many of the models have similar phases and approaches; and some models focus of certain areas of investigations that is needed by their environments. Figure 1 illustrates our suggested digital forensics model that is based on the chain of custody concept.

The ultimate objective of digital forensics is to secure solid evidence that will point to the person or persons responsibility for the cyber crime. We suggested the container or the digital bag to preserve all our evidences, We proposed a framework with following phases:

1. Identification

Identification is identify elements or devices that may include: computers, mobile phones, tablets, or any other storage device that may contain digital information, the network also and identified cyberspace

2. Acquisition:

Then acquisition is done by seizing electronic devices found in the crime scene and forensically obtaining the digital data found and exactly duplicating and isolating the for investigation purposes.

3. Preservation/Storage:

After the evidence have been acquired it shall be kept isolated and as it is. There should be a concrete chain to preserve the evidence from been altered. Images or read only copies should be kept in this stage.

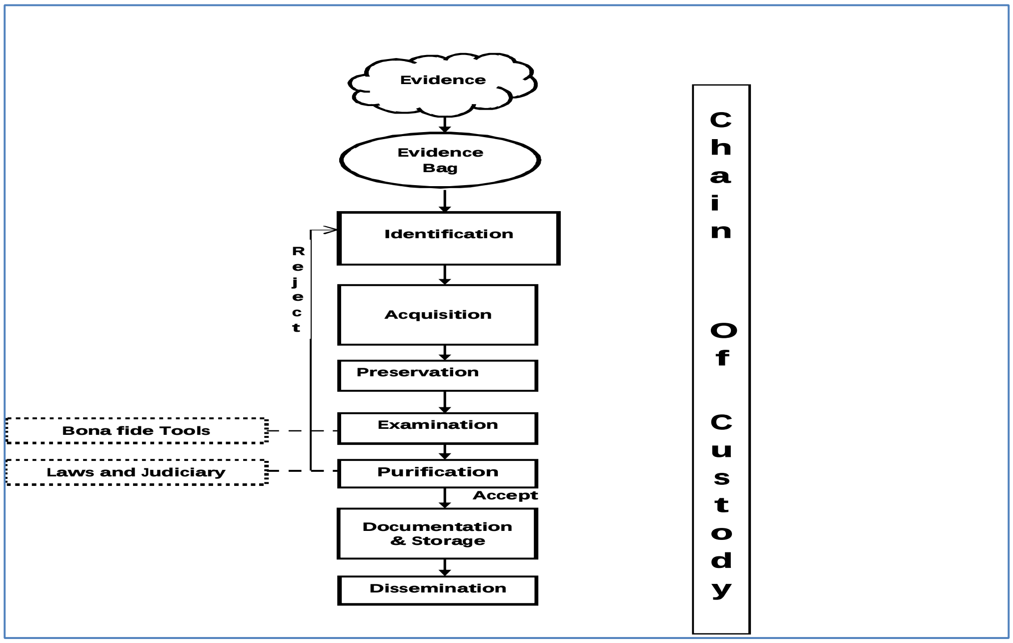

Figure 1: Digital forensics model that follow the chain of custody procedure

1. Examination:

In this stage we examine and analyze the evidence preserved in the previous step. The tools mentioned in Table 2 or any other tools should be used in this stage to solidify the digital evidence. The evidence extracted for instance from e-mails message can be compare with image files preserved. The analysis step begins by identifying the methods, tools, and skills needed for extracting vital information that can be used in the judiciary system. In this examination stage we suggest a technical committee to approve the digital forensics software or hardware and then certify these software as a bona fide software and hardware. Sammons [19] described in a whole section in his book how to validate forensics software and hardware. Forensics personnel in this stage must be well trained in Technology and Law to conduct their job in a professional manner

2. Purification:

Evidences must be reviewed using the laws and acts in place. Reviewing and normalizing these digital evidences with laws and acts available in the system will make these digital wvence acceptable in the judiciary system in the state.

3. Documentation/Presentation

The examiners shall provide and present a report. The report should document the way how the foresnic process took place, point any odd events if existed, and tools and methods used. The protocols, policies, and legal aspects followed. the writing and the presentation of the report should be understood, consistent, and appealing. The facts and findings should be accurate and clearly presented.

4. Dissemination:

There should be a clear policy concerning the broadcasting and dissemination of the information concerning all the above stage of this digital forensic processes. Not all information may be released but essential information must be as a feed to other digital cases.

5. CONCLUSION

In this work, a complete digital forensic framework with all its processes have been suggested. the frameworks enhanced with many aspects from technology and laws. The concept of chain of custody has been utilized to formulate this digital forensic model or framework. The digital forensics tools is handled in a way that it should be tested and verified and classified as bona-fide. The training of the investigation team is crucial since dealing with advanced technologies and sophisticated acts of law is a challenging process. The model is expected to suit Sudan judiciary system

6. RECOMMENDATIONS FOR FUTURE WORK

The limitation of this research resides on that real Sudanese court data is not used in a big scale or as a big sample. A survey that uses several cybercrime cases with the key actors be involved will show the weaknesses and the strengths of the model or the framework.

ACKNOWLEDGEMENTS

The authors would like to thank International University of Africa, Khartoum, Sudan, for assistance they rendered concerning this work.

References

[1] Thomas J. Hol, Adam M. Bossler, t, Kathryn C. Seigfried-Spellar (2017)"Cybercrime and Digital Forensics: An Introduction". Routledge; Second Edition

[2] Casey, E.: Digital Evidence and Computer Crime, 2nd Edition, Elsevier Academic Press, 2004.

[3] . Kshetri, N.(2010) The Global Cybercrime Industry. Berlin, Heidelberg: Springer Berlin Heidelberg.

[4] Harbawi, M, Varol, A. "The role of digital forensics in combating cybercrimes." Digital Forensic and Security (ISDFS), 2016 4th International Symposium on. IEEE, 2016.

[5] Kent, K, S. Chevalier, T. Grance, H.Dang (2006) "Guide To Integrating Forensic Techniques Into Incident Response." NIST Special Publication 10 (2006): 800-86.

[6] Nirkhi, Smita, R. V. Dharaskar, and V. M. Thakare.(2015) "An Experimental Study on Authorship Identification for Cyber Forensics." IJCSN International Journal of Computer Science and Network, Volume 4, Issue 5, October 2015 ISSN (Online) : 2277-5420 www.ijcsn.org

[7] Umesh Kumar Singh, Neha Gaud , Chanchala Joshi (2016) A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity. International Journal of Computer Applications (0975 – 8887) Volume 154 – No.6, November 2016

[8] Reith, M., Carr, C. and Gunsch, G.:An Examination of Digital Forensic Models, International Journal of Digital Evidence. Fall 2002, Volume 1, Issue 3, 2002.

[9] Ciardhuáin, SO.: An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004.

[10] T. F. Gayed, H. Lounis, and M. Bari, "Computer Forensics: Toward the Construction of Electronic Chain of Custody on the Semantic Web," in Proc The 24th International Conference on Software Engineering & Knowledge Engineering, pp. 406–411, 2012.

[11] J. Rajamäki and J. Knuuttila, "Law Enforcement Authorities ' Legal Digital Evidence Gathering," in Proc European Intelligence and Security Informatics Conference, pp. 198–203, 2013.

[12] K. Lim and D. G. Lee, "A New Proposal for a Digital Evidence Container for Security Convergence," in Proc IEEE International Conference on Control System, Computing and Engineering, pp. 171–175, 2011.

[13] [1] Bobbler.M.M, Solms S.H.von. Modelling Live Forensic Acquisition, Workshop on digital Forensic Incident analysis (WDFIA 2009).

[14] [2] R.Ieong FORZA digital forensics investigation frameworkthat incorporates legal issues,Digital Investigation. Volume 3, Supplement 1. P 29 – 36

[15] [3] Vlachopoulos.K., Magkos S.E., and chrissikopoulous V.AModels for Hybrid Evidence Investigation International Journal of Digital Crime and Forensics 4(4):47-62. DOI: 10.4018/jdcf.2012100104

[16] Jasmin Cosicand Zoran Cosic (2012) Chain of custody and life cycle of digital evidence. Computer Technology and Application 3 (2012) 126-129

[17] Tabona, A (2018) Top 20 Free Digital Forensic Investigation Tools for System Administrators. https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

[18] https://github.com/

[19] Sammons, J.(2012). The basics of digital forensics : the primer for getting started in digital forensics. Syngress, Elsevier, Inc. ISBN 978-1-59749-661-2