American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Computer & Cyber Forensics: A Case Study of Ghana

Mohammed Mahfouz Alhassan[a*], Alexander Adjei-Quaye[b]

[a,b]*Zhejiang Normal University, College of Mathematics, Physics& Information Engineering 688 tying bin road, Jinhua Zhejiang Province 321004, China*
[a]*Email: mmalhassan@tamalepoly.edu.gh*
[b]*Email: adjeiquayealexander@gmail.com*

Abstract

The study was to examine the importance for the study of computer and cyber forensics in the fight against crime and prevention of crime. Using the security agencies in Ghana namely the Ghana police service and the bureau of national investigations. Information and Communication Technology (ICT) is at the center of the world today. The applications and concepts, techniques, policies and implementation strategies to security services has become a subject of fundamental importance and concerns to all security agencies and indeed a prerequisite for local and global competitiveness. The purpose of the research is to assess and evaluate the impact of computer related crimes on the continent of Africa and especially Ghana in particular. The Bureau of National Investigations, (BNI), to find the positive and negative impact of ICT and its related contributions in the everyday life of Ghanaian security agencies, especially the BNI and GPS ones(once) to examine how ICT has helped reduce and prevent crime and also cost of identifying and preventing crimes thus to determine the efficient use of information technology to help fight corruption at workplaces, prevent and protect the country and its people from any kind fraud within or attached that will be launched on the Ghanaian soil using ICT.

Keywords: Computer and cyber forensics fundamental importance and concerns to all security agencies.

1. Using the proxy or VPN server to commit an offense

A proxy server is a computer hardware system or a computer software application that acts as an intermediary for requests from clients seeking resources from other servers. When a client connects to a proxy, asking for some services such as a file, connection, web page, or another resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

---

* Corresponding author.

Proxies were invented to add structure and encapsulation to distributed systems. Most proxies are web proxies, enabling access to content on the World Wide Web and providing anonymity for the user, this anonymity helps the user to either commit a crime or prevent a crime from being committed, it also helps expose a crime that is being committed or has been committed.

In the United states Corporations routinely use proxies to enable their employees to work from home; virtual private networks, or VPNs, make traffic look like it's coming from within the company's internal network, thus bypassing its security firewalls without a trace [10].

Cell phone providers use proxies to connect devices to the Internet, while people in repressive countries use them to circumvent Internet censors. Internet service providers(ISP) also use proxies to speed traffic, by storing copies of frequently accessed Web pages locally, avoiding the need for users to reach out to the original site every time.

Privacy-minded users also rely on proxies to surf the Internet anonymously. With the free service Tor, for example, people install software to turn their computers into relay points for routing traffic between other people's computers. Thus, a Web site only knows the identity of the last relay point, not the user actually accessing it.

But such anonymity proxies can be used for both good and bad, and a debate is stirring as the government of U.S and others proposes to impose stiffer penalties for crimes committed by someone who had been using those and other proxies.

The U.S. Sentencing Commission is scheduled to vote on a series of amendments to the sentencing guidelines, which heavily influence the sentences that judges hand down. This kind of amendment in question would treat the use of proxies as evidence of "sophistication" in planning certain types of crimes, from embezzlement to forgery and other types of fraud and terrorism-related crimes.

If the commission approves it, the change takes effect unless the U.S Congress takes the rare step of blocking it beforehand.

Opposing the change requires a delicate touch because the rule would apply only to people already convicted of crimes and facing sentencing.

Many lawmakers think It kind of a fine line that needs straightforward approach believing it will serve as a deterrent to cybercriminals. but other lawmakers also think the government shouldn`t be creating and institutionalizing a disincentive, a penalty for routine, safe privacy practices.

2. Forensic Data Collection

The forensic data collection table below lists the processes to be followed during the data collection.

Physical	Logical	File system
Bit-By-Bit image of the device	Active content (User accessible)	Active content with application support
Includes deleted data	Does not include deleted data	Partially recovers deleted data
Captures call logs, sms, mails, Application data and Images, music and videos	Captures only active content like contacts, call logs, Images, music and videos	Captures contacts, call logs, Images, music, videos, and Application data

Figure 1: Forensic data collection table.

Legal Backing for Computer Forensics in Ghanaian Court System

Forensics or systems security experts overseeing network security must be aware of the legal implications of their forensic works and activities. These security experts need to consider their policy decisions and technical responsibilities, actions in the context of existing laws. For instance, you must have authorization before you monitor or conduct any form of forensics auditing or investigation and collect information related to a computer intrusion, detection or offense.

Computer forensics is a relatively new discipline to the courts and especially developing countries, and many of the existing laws used to prosecute computer-related crimes, lacks the legal backing precedents especially in countries where there are limited professionals in the field of forensics, and practices related to computer forensics are in a state of flux. Example new courts rulings are issued that affect how computer forensics is applied.

The research lists recent court cases involving computer forensics and computer crime related cases in the United States, and it has guides about how to introduce computer evidence in court and what standards apply. Forensics experts and investigators have helped nations around the globe to help retrieve and put behind bars, people that uses the computer or the internet to steal and conceal vital information's that cause nations billions of dollars of the taxpayer's monies.

The important point for forensics investigators is that evidence must be collected in a way that is legally required and can be admissible in.

Nations around the world are increasingly introducing laws ad also laws are being passed that require organizations to safeguard the privacy of personal data. It is becoming necessary to prove that your organization is complying with computer security best practice most especially government institution in the developing countries, where most people think you can rob the state with the computer without been caught, because it's believed that, the states lack the required forensics expertise to investigate and prosecute cases in the law court. So if there is an incident that affects critical data, for instance, the organization that has added a computer

forensics capability to its arsenal will be able to show that it followed a sound security policy and potentially avoid lawsuits or regulatory audits.

And developing like Ghana need to study the united states laws that establish computer security laws to give it the backing and help protect and defend the country against computer espionage, computer theft and so on.

If digital evidence survives the Daubert challenge, it may still have to surmount several competency hurdles concerning the collection, storage, processing and presentation of the evidence to the courts. Computers today come with or can be augmented to provide huge amounts of data storage. Gigabyte disk drives are common and a single computer may contain several such drives. Seizing and freezing can no longer be accomplished simply by burning a single CDROM [9]. Failure to freeze the evidence prior to opening the files, coupled with the fact that merely opening the files changes them, can and has invalidated critical evidence. Then comes the problem of locating the relevant evidence within massive amounts of data. Wading through such volumes of information to find relevant evidence is a daunting task. As daunting as these problems are, additional problems arise when we have to look beyond a single computer. In modern distributed computer architectures, the digital evidence we need may reside on many different servers and clients within the organization's IT infrastructure. The problems get even more difficult when the IT infrastructure is connected to the Internet, for then digital evidence may be spread across vast geographic distances and several sovereign jurisdictions.

3. Physical Crime Scene

One of the most important aspects of securing the crime scene is the preservation of the scene to ensure there is minimal or no contamination and disturbance of physical evidence. The initial response to an incident shall be expeditious and methodical [7]. Upon arrival, the officer(s) shall assess the scene and treat the incident as a crime scene if a crime is established to have taken place. Policy: The initial responding officer(s) shall promptly, yet cautiously, approach and enter crime scenes, remaining observant of any persons, vehicles, events, potential evidence, and environmental conditions.

- Procedure: The initial responding officer(s) should: a. Note or log dispatch information (e.g., address/location, time, date, type of call, parties involved).
- The responding officers/officer should be aware of any persons or vehicles leaving the crime scene.
- The officers should approach the scene cautiously, scan the entire area to thoroughly assess the scene, and note any possible secondary crime scenes. Be aware of any persons and vehicles in the vicinity that may be related to the crime.
- Make initial observations (look, listen, smell) to assess the scene and ensure officer safety before proceeding.
- The officer should always remain alerted and attentive. Assume the crime is ongoing until determined to be otherwise.
- Treat the location as a crime scene until assessed and determined to be otherwise

In the physical crime scene, the preservation of the entire crime scene is very important to avoid taking evidence that is tainted, most importantly if the crime took place in an open place, it will be better to cordon it off, with a

tape, objects or human wall to and make sure there is a distance between the forensic investigators and witness or spectators. Also taking of visual images should be giving most priority because every investigation might end up in the court system, therefore picture images should be given the top most priority.

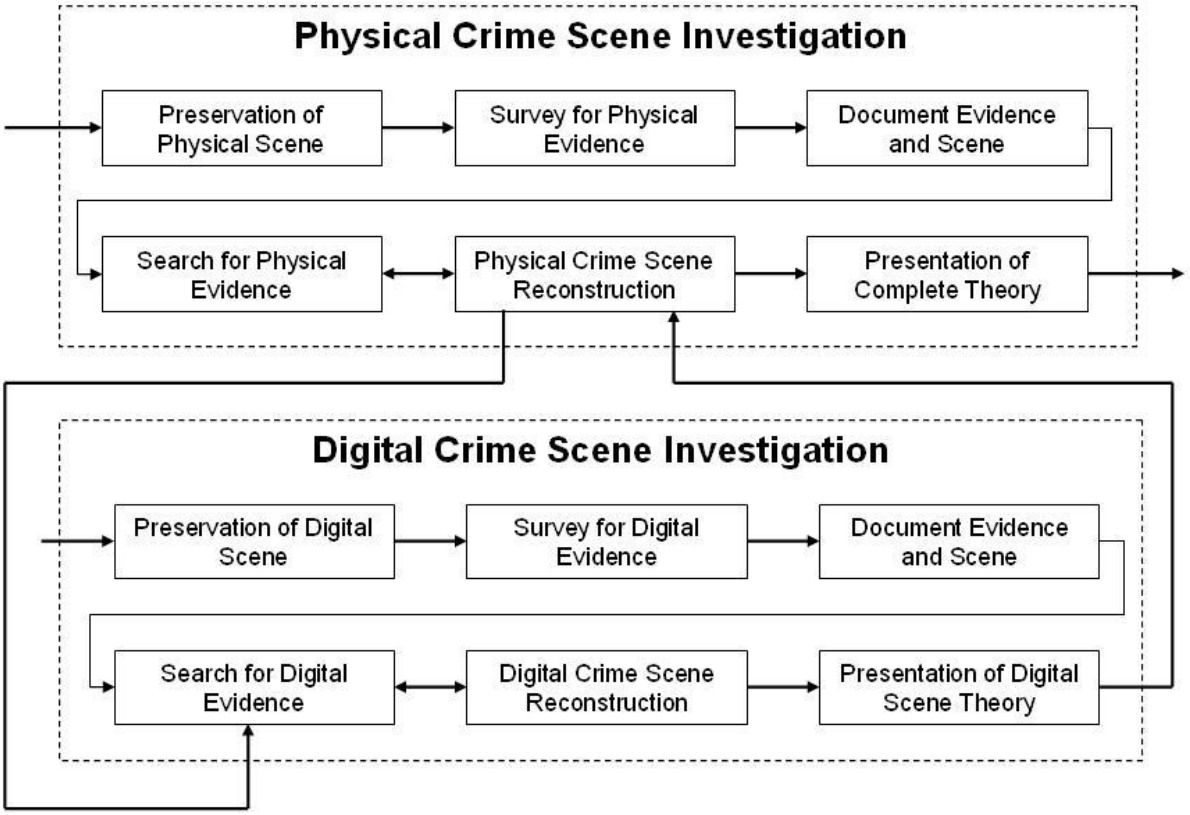

Figure 2: Crime scene table

4. Digital Crime Scene and Evidence

Digital crimes scenes are normally crimes that take place in homes, office or maybe places that are not too open, preservation of the digital devices thorough scrutiny of whatever digital device is available or near the crime scene, documentation of each and every step taking, searching for every piece of evidence available on the device, try reconstruction the whole crime as you are likely to come out with some of the possibilities that helped in committing the crime and document each and every step. The documentation should involve both writing text and still images that can lead to a successful identification and prosecution. Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. This evidence can be acquired when electronic devices are

Seized and secured for examination, Digital evidence: Is latent (hidden), like fingerprints or DNA evidence

• Crosses jurisdictional borders quickly and easily

• Can be altered, damaged or destroyed with little effort [5].

Internet-based computers and devices, stand-alone computers or devices, and mobile devices. Some of these areas tend to have different evidence gathering processes, tools and concerns, and different types of crimes tend to lend themselves to one device or the other.Example, Photo search application finds digital images that satisfy certain conditions. Photo search application shows the query form that is presented to users. An investigator can select the camera model that was used to record the image, the date/time on which the recording took place, the resolution of the image, etc. For brevity, we omit the underlying query template. The query constructed from that template combines file-system metadata and EXIF information extracted from digital images. The query produces XML region nodes and some additional metadata. The query result includes image previews which are generated by requesting the relevant regions from the virtual BLOB server. One thing about digital forensics is that it appeals to many practitioners is the social contribution of serving the criminal justice system or another system such as national defense. Another thing about digital forensics that is so appealing to many is that every case is different. Investigating human misuse of computers creates new puzzles and technical challenges, particularly when offenders attempt to conceal incriminating evidence and their activities on computer systems and networks. In addition, the growing demand for qualified practitioners also makes digital forensics an attractive career choice for many.

This growing interest and need have sparked heated debates about some of the tools, terminology, definitions, standards, ethics, and many other fundamental aspects of this fast developing field**[8]**. It should come as no surprise that this research reflects diverse positions in these debates. Most notably, this text reflects not only my belief that this field must become more scientific in its approach. Mobile devices perform different an array of functions ranging from a simple telephony device to those of a personal computer. Designed for mobility, they are compact in size, battery-powered, and lightweight. Most mobile devices have some basic set of comparable features and capabilities [6]. They house a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces and a liquid crystal display (LCD). The operating system (OS) of a mobile device may be stored in either NAND or NOR memory while code execution typically occurs in RAM. Currently, mobile devices are equipped with system-level microprocessors that have the functions to reduce the number of supporting chips required and include considerable internal memory capacity currently up to 64GB (e.g., Stacked NAND). Built-in Secure Digital (SD) memory card slots, such as one for the micro Secure Digital eXtended Capacity (microSDXC), may support removable memory with capacities ranging from 64GB to 2TB of storage. Non-cellular wireless communications such as infrared (i.e., IrDA), Bluetooth, Near Field Communication (NFC), and WiFi may also be built into the device and support synchronization protocols to exchange other data (e.g., graphics, audio, and video file formats).

(Acquiring and Evidence Handling the Procedure)

Before acquiring forensic evidence from a computer, it’s important for the forensics investor to ensure the system is powered on and not turned off.

- A computer forensic specialist or forensic investigator should be consulted when available.
- Before powering down a computer, it is important to consider the potential of encryption software

being installed on the computer or as part of the operating system and also keep in mind that some vital information, may be kept in the computer memory, and the function of the computer system memory is handled data for a few seconds, so if a forensics expert or /investigator is present, the appropriate forensic methods should be utilized to capture the encrypted data before the computer is powered down.

- It's very important for the forensics expert to assess and ensure that the power needs for the devices with volatile memory and follow agency policy for the handling of those devices.
- Documentation of every step during the forensic investigation is unique for success prosecution of purposes because the forensic expert may be required to explain to courts about some of the processes and procedures followed or taking during the audit, or investigation so, documentation in every step of the forensics ingestion is so essential.
- Take legible photographs (screen, computer front and back, and area around the computer to be seized) and/or make a sketch of the computer connections and surrounding area. Also, ensure noninterference doing the forensic process. Using XIRAF, have implemented a number of small but useful forensic applications. These applications have been tested in several cases; the size of the disk images in these cases ranged from 40 to 240 GB. The applications cover a range of functions – browsing, searching, and knowledge bases – and illustrate the versatility of our query-based approach. Forensic investigators, however, need not be familiar with the XQuery language; they access the XIRAF applications through simple web interfaces[3].
- Appropriately document the connection of the external components this includes both flash drives, memory cards and so on.
- Remember to document any pre-existing damage to the evidence.
- Affects taking the critical data evidence generation that has added a computer forensics capability to its arsenal will be able to show that it followed a sound security policy and potentially avoid lawsuits or regulatory audits.
- There are some important areas of law related to computer security that is important to know about that forensics are supposed to know, though.

During evidence analysis the process of interpreting the extracted data can determine their significance to the case. Some examples of analysis that may be performed during the process will include and not limited to timeframe, data hiding, application and file, and ownership and possession. The analysis may require a review of the request for service, legal authority for the search of the digital evidence is very essential, because it affords you the rights to exercise your authority and to perform your duties without fear, of the stature of the individual investigate gated lead [2].

5. Need for Computer and Digital forensics Policy in developing Countries

Digital and Computer forensics as a discipline demands specially trained people, and support from governments and agencies, and the necessary funding to keep the forensics unit operating. This can be achieved by constructing a comprehensive training program for examiners and also introducing policies that will encourage sound digital evidence recovery techniques and a commitment to keep any developed unit operating at

maximum efficiency [4].

In most part of the world today, especially in developing nations where the use of computers and other digital devices are been used daily on the internet for fraudulent activities, this kind of laws will help in eradicating and minimizing computer related crimes being committed by both the educated class and the young future leaders of various countries that get the feeling that, their only way to riches is to sit behind the computer and engage in cyber fraud, because they are aware of the lack of laws, policies and technical manpower to investigate and prosecute computer-related crimes.

6. Ransomware

Hospitals, health centers, universities,colleges, districts and metropolitan assemblies , state and local government institutions , law enforcement agencies, small businesses, large businesses establishments—these are just some of the entities impacted by ransomware, an insidious type of malware that is capable of encrypting, or locking, valuable digital files and demands a ransom it will be released**[1]**.The inability to access this kind of important data, that these organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses will be incurred to restore systems and files, and the potential harm these can cause to an organization's reputation. Home computers are just as susceptible to ransomware and the loss of access to personal data and often irreplaceable items— including family photos, videos, and other and other important data—can be devastating for individuals as well.

In a ransomware attack, the victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears deceptive or legitimate to the user, like an invoice or a pay cheque or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

7. Conclusion

In conclusion, the research work identifies some Existing general purpose computer forensic analysis tools that are rapidly been used for modern-day forensic investigation. The outdated – first generation – architecture restricts their ability to scale and accommodate current and future analysis requirements. In recent years researchers have cited the need for more capable forensic analysis tools and proposed the use of Beowulf clusters to deliver greater processing capability. While this is a valuable advance in the successful discharge forensic of all forensic, the research also found the need for the need of more forensic investigator in Ghana and other less developed countries, that are been robbed my these that are put in at the helm of the affairs of those nations, to help build the next generation of leaders with integrity. It's important to train forensics investigators can`t be compromised, and also setting up of more forensics labs, to help in the successful ton computer forensic tools were discussed. Requirements for second generation tools have been proposed. An early high-level design for a practical second generation computer forensic analysis system was presented. Design and implementation work on this system is ongoing. The system includes novel strategies for optimizing and managing evidential data, managing and need for the due process of the evidence gathering. Computers and grid computing

resources for computer forensic analysis. Once the proposed second generation system has been implemented, tests will be conducted to quantify its performance in terms of the metrics discussed above. The value of developing standardized tests and analysis strategies, implemented in open-source and reusable software modules widely accepted by Courts and the analysis community, was reiterated.

Another most important discovery was the need for more forensic expert, and the latest forensic equipment's, that will help in the speedy analysis, legal backing that gives the forensic experts go after whosoever has in one way or the other dip his hands in the state's coffers. This is needed because, the developing countries are the places where most robberies of the states monies are being stolen and the people that are supposed to protect the states and ensure the states has the monitoring tools in both human materials resources, because this person thinks by empowering the security agencies to fight crimes are the same people that steal using the computer and the internet, because they know in doing that, they can never be found or hunt down and the affordability of this courses will propel more people to take interest in this all-important career.

This will help redirect the youth of this parts of the world that thank they can use the computer and the internet to rob people not only in Africa but around the world without being caught.

Acknowledgement

Our greatest thanks go to Professor, Han JianMin with Zhejiang Normal University, College of mathematics, physics, and information engineering for his excellent supervisory guidance, skills, and help, and more importantly guiding us through each and every step of the process with knowledge and support. Thank you for your advice, guidance, and assistance. The management and staff of the college are not left out for their support in making this research a success. We say thank you very much.

8. Support

This work is supported by National Natural Science Foundation of China under Grant 61672468.

References

[1].United States Department of Justice's Cyber Crime website. Retrieved from http://www.cybercrime.gov.

[2] United States Department of Justice. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved from. http://www.cybercrime.gov

[3] Wouter Alink, Raoul Bhoedjang, Peter Boncz, and Arjen de Vries. From the proceedings of The Digital Forensic Research Conference DFRWS 2006 USA Lafayette, IN (Aug 14th - 16th)

[4] U.S. Department of Justice Office of Justice Programs, National Institute of Justice, NIJ Special report.April (04)

[5] A Simplified Guide To Digital Evidence, ELECTRONIC CSI, A GUIDE FOR FIRST RESPONDERS,2ND EDITION, National Institute of Justice, April 2008

[6] Rick Ayers Sam Brothers Wayne Jansen, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1, May 2014

[7] U.S. Department of Justice Office of Justice Programs National Institute of Justice, crime scene investigation, A Guide for Law Enforcement A Guide for Law Enforcement, research report. January 2000

[8] Casey, Eoghan. Digital evidence and computer crime: forensic science, computers, and the internet, with contributions from Susan W. Brenner 3rd edition.

[9 Daniel J. Ryan, Gal Shpantzer, Legal Aspects of Digital Forensics,

[10] Jordan Robertson, U.S Mulls stiffer sentences for, Net proxy crime, Associated press updated 4/14/2009 1:17:14 PM ET