BOOK CHAPTER | *"It takes the right tools""*

Tools For Cyber Forensics

Peter Oppong Baafi
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: peeuncle3@gmail.com
Phone: +233242776968

ABSTRACT

Digital forensics, or Cyber security, has become a vital part of almost every research, and digital forensics tools' users are becoming more diverse in their backgrounds and interests. As a result, usability is an important section of these tools. This paper investigates the usability aspect of forensics tools. The study results highlight several usability issues that need to be considered when designing and implementing digital forensics tools. Cyber-attacks are fast-moving and surging in number and severity. When the attacks occur, the attacked enterprise responds with predetermined actions. Applying digital forensics helps in recovering and investigating material on digital media and networks is one of these actions. Cyber Forensic Investigation includes the Capture and Analysis of digital data either to prove or disprove whether the internet-related theft has been committed or not. Earlier, Computers were used only to store large volumes of data and perform many operations on them, but nowadays, it has expanded and occupied a prior role in Crime Investigation. To solve these cyber-related problems, the selection and usage of Forensic tools are essential. The developers have created many cyber forensic tools for better research and quick investigation. Cop departments and investigation agencies select the tools based on various factors, including budget and available experts on the team. This paper describes the different types of existing computer forensic tools and their usage. The article gives detailed information on all related works by other scholars in the area of this paper.

Keywords: Digital Forensics; Forensics, GUI, User Interface, Digital Forensics, and its framework, Cyber forensics tools.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Peter Oppong Baafi (2022): Toosl For Cyber Forensics
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 285-290
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P46

1. INTRODUCTION

Digital forensics tools play a vital role in providing reliable computer analysis and digital evidence collection to serve legal and industry purposes. These tools are used to conduct computer crime investigations by identifying evidence that can be used in a court of law. In addition to the

criminal investigation, these same tools are used for maintenance, error-finding, lost data recovery, and reverse engineering of information systems in private jurisdictions.

Digital forensics is rapidly becoming a substantial part of computer investigations worldwide, used by law enforcement and private organization investigators. Digital forensics tools are crafted for use by forensics investigators. Considering these users' backgrounds, computer expertise, workflow, and practices. In practice, users might have any knowledge in IT, ranging from computer security experts to criminal investigators possessing basic computer skills. With this varied range of computer expertise, practitioners need "usable" tools that will help them get results efficiently. Humans prefer to focus on a given task for a finite amount of time to achieve specific goals. When interrupted by distractions, individuals become confused or complacent and distracted from their primary goal. When examiners investigate digital forensics, they typically seek answers to specific questions they perceive. Practitioners often do not care about any technical details that divert them from their two primary goals: investigative pieces and conviction support.

Practitioners may claim to be certified tool users even when giving witness statements in court instead of experts who understand how a tool works. Digital forensics is a part of forensic science encompassing the recovery and investigation of material found in digital devices, often concerning computer crime. Computer forensics is also known as cyber forensics. It involves applying computer investigation and analysis techniques to solve a crime and provide evidence to support a case. It is the phenomenon of identifying, preserving, analyzing, and presenting digital evidence so that the proofs are legally acceptable. By using cyber forensic tools, it is straightforward to probe the evidence. It involves various applications like analyzing food quality and predicting fire disasters etc. This paper investigates digital forensics tools' validity, usability, and application in present-day digital forensics.

1.1 Background

The usability of forensics tools is becoming an essential aspect of any technical device. The international standard ISO 9241-11 explains usability as: "The extent to which specified users can use a product to obtain specified goals with effectiveness, efficiency, and satisfaction in a specified context."The usability of computer systems is considered an important area of research and is often a metric used to evaluate procedures. Therefore, usable security is a vital and strategic study area. The field of usable security targets the application of computer security tools user-friendly. The research in this section interests academia and professional practitioners and serves government institutes and private organizations. In the past 30 years, cyber forensics has migrated from a very ad-hoc and possibly destructive use of system administration tools to a formal phenomenon utilizing specialized tools.

Technological upgrades in court cases have created a need for reliable digital forensics tools. Today these tools can make best-evidence copies and perform non-destructive data analysis. Contemporary analysis can uncover deleted files, construct event timelines, attribute events to users, etc.(ASCLDLAB). American Societies of Crime Laboratory Directors Laboratory Accreditation Board "recognized digital evidence as a full-fledged forensic discipline” in 2003. Also, the interest in training and education has grown, causing many universities and training institutions to offer a range of computer forensics courses and degrees where students can gain in-depth expertise in digital forensics.

Fig 1: Tools for Cyber Forensics
Source: https://ifflab.org/list-of-15-most-powerful-forensic-tools/

2. RELATED LITERATURE

M. Reith et al.(2002) propose abstract models as a possible replacement for existing forensic models that seem too specific. The authors also observe that existing digital forensics tools are typically too technology-specific, becoming inconvenient for non-technical users. Such users generally have been given enough training to use a particular device but may not have any primary education about the underlying technology employed by the tool. Modern digital forensics tools use several specific, complex technologies. This complexity causes the creation of specialized classes and books dedicated to the subject. Even though the goal of these classes and readers is to provide a technical foundation for forensics examiners to use their tools better, these information sources gear towards very low-level topics that are usually ancillary to an investigator. S. Garfinkel (2010) investigates trends in forensics research and observes that the field is likely "to fall behind" shortly.

Current forensics tools were made in an "evidence-oriented" manner. The author explains that this way of developing digital forensics tools has created some of the challenges users face today. J. Farrell (2009) addressed several issues with forensics tools involving usability and proposed a fresh approach to forensics reporting. Regardless of the current manual method that relies on a trained human operator, the author has suggested a digital tool to "perform automated analysis and issues reports."

Furthermore, he proposed design components for an automated reporting tool framework that considers three core categories: systems, user interface, and reporting intelligence. The study emphasized making the tool more efficient for untrained users by following a "user-centric approach that requires minimal human involvement, increasing usability and providing results with less time and effort.

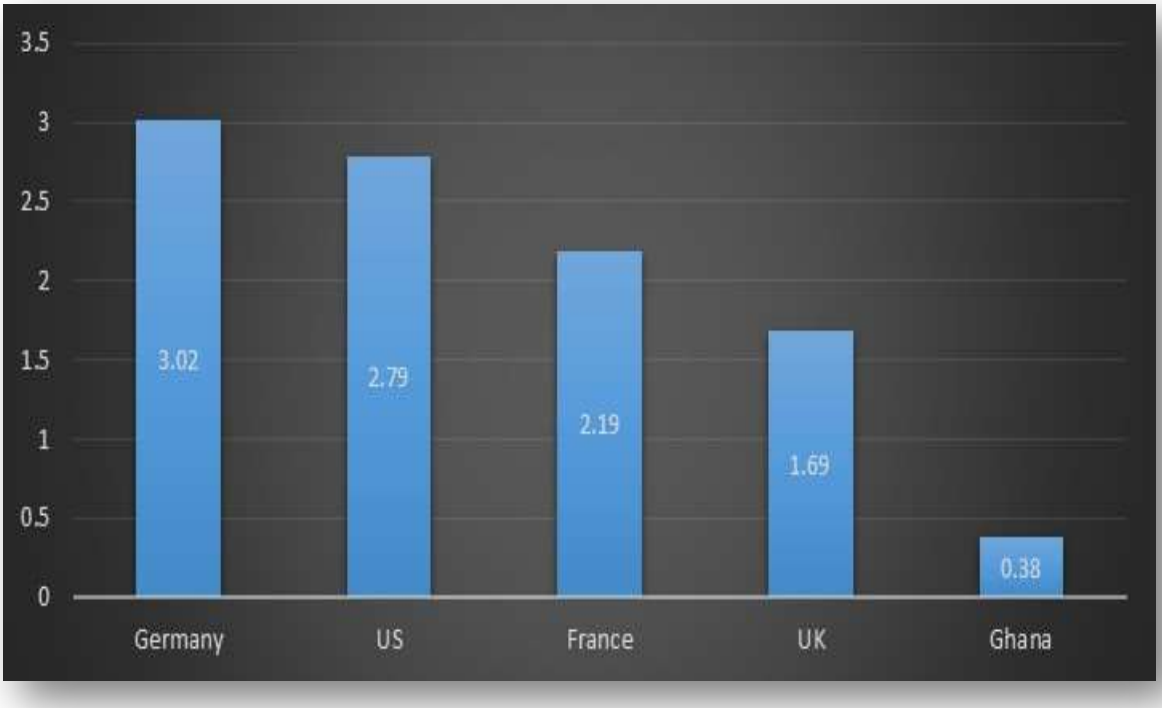

Fig 1: Overview of the digital forensic infrastructure of Countries by Comparism
Source: International Telecommunication Union - ScienceDirect.com

3. RESEARCH GAPS/FINDINGS

The paper's results provide strong evidence that current digital forensics tools are not considered user-friendly and lack intuitive interfaces. It is a challenge for investigators to find answers to their high-level, case-related questions directly. Usability is crucial in these tools because misunderstanding that leads to false interpretations may impact real-life cases. Currently, users are overwhelmed with the technical background required to use these tools. Indeed, there are cases where an investigator needs to understand computer systems and networks to interpret the evidence correctly. However, this is not always required.

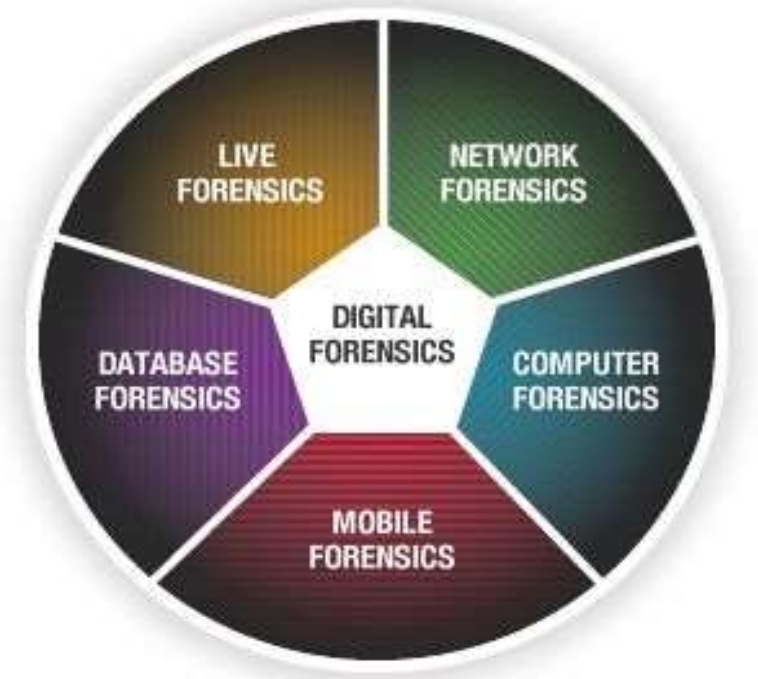

Fig 1: Types of Forensics
Source: https://www.pinterest.com/chang_pie/cyber-forensics/

According to knowledge gathered, it is usually the case that field agents are investigating to get answers to simple probing questions such as: "Did culprit A contact Person B on that date? What websites did he browse? What kind of emails did he send and with whom?" When field agents are faced with issues involving technically savvy criminals, they generally ask more experienced personnel to examine the evidence.

Therefore, it is essential to keep all levels of users in perspective. Designers of these tools should be mindful of the Microsoft Office, for example, where users of different expertise standards can make the reliable use of the software: an amateur user can easily find his means of writing a letter or report also, and a more sophisticated user will make use of advanced tools the program offers (such as writing macros or connecting to an online collaborative repository).

4. CONCLUSION

My goal is to outline a set of usability frameworks for designing digital forensics tools. System designers and software engineers can use these guidelines to implement software solutions that meet the needs of digital forensics practitioners. This paper helps to show a few existing and popular digital forensics tools used by various experts in digital forensics in performing various forensics investigations. This field will enable crucial electronic evidence to be found, whether lost, deleted, damaged, or hidden, and used to uncover records or information deemed to be failed.

5. RECOMMENDATION FOR POLICY AND PRACTICE

We recommend that available forensics tools capable of simplifying forensics activity and more reliable be made available to all levels of forensics tools users. The usability of these tools should not be the one that may pose complexity and user-unfriendliness. Experts in digital forensics must equip themselves with the usability of the current available sophisticated or less complex cyber forensics tools. The usability of cyber forensics tools currently seems to be one of the significant fallbacks to the accuracy and trustworthiness of cyber forensic results. Having a policy line that requires all experts in the area to be well-acquainted with the emerging tools is the way to expand the landscape for the usability of cyber forensics tools.

6. IMPLICATIONS FOR CYBER SECURITY IN AFRICA, POLICY, RESEARCH, AND PRACTICE

Appropriate cyber security infrastructure usage has reliable and secure data protection and use. The lack of standard and state-of-the-art cyber security policies and infrastructure possesses significant data and transactional insecurity. Africa and its communities must learn to adopt adequate and reliable cyber security tools.

Without these infrastructures in place, the data hubs and centers that generate and use big data and all forms of data stand so slippery to data theft or corruption in the times unknown to come. Adequate research works in the area of cyber security will help to improve the available infrastructures. This infrastructure, if upgraded, put Africa in the correct position to run policies capable of subverting all cybersecurity-related threats or issues in the area of data usage and its management in the Africa sub-region.

7. DIRECTION FOR FUTURE WORKS

In this paper, I have reviewed some of the areas that need improvement: reporting, graphics, user interface, and collaborative environment, among others. I plan to expand this research to explore many of these areas and conduct more user testing to better insight these problems. Future researchers can complete a more extensive survey to better understand the digital forensics tools landscape.

REFERENCES

[1] S. Garfinkel, 2010, "Digital forensics research: The next ten years," Digital Investigation, vol. 7, pp. S64–S73.

[2] J. Farrell, 2009, "A Framework for Automated Digital Forensic Reporting," Master's thesis, Naval Postgraduate School, US.

[3] L. Cranor and S. Garfinkel, 2005, Security and Usability: Designing Secure Systems that People Can Use. O'Reilly Media, Inc.

[4] B. Carrier, File system forensic analysis. Addison-Wesley Professional, 2005.

[5] SANS Investigative Forensics Toolkit SIFT Available:http://digitalforensics.sans.org/community /downloads