BOOK CHAPTER | *"What a Way – X-Ways"*

X-Ways Forensics Platform For Digital Forensics Examiners

Seth Adjei Gyimah
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mails: sethadjeigyimah@gmail.com/ seth-adjei.gyimah@st.gimpa.edu.gh
Phone: +233244475540

ABSTRACT

Crime has evolved over the years from its traditional form to digital crimes. Those who commit such crimes use advanced and sophisticated tools, equipment and techniques to perpetuate such crimes. In order to effectively and efficiently investigate, examine and gather evidence from such complex crimes, digital examiners have to employ various tools and techniques to analyze, extract and recover data as evidence to assist in prosecution of the perpetrators of the crime.
This paper analyzes X-Ways Forensics platform which is an application software for forensic examiners as a forensic tool for data extraction, analysis and recovery. Dr. Larry Leibrock, Founder and CTO of eForensics revealed his admiration for X-Ways Forensics application when he said "As a professional forensics examiner, I have used X-Ways Forensics as a forensics instrument in recovering and analyzing digital information. I have tested and validated the professional version and it has proved to be accurate and trustworthy in its reporting. I have the highest level of confidence in X-Ways Forensics efficacy in digital forensics cases. I am confident that the tool and my use of this instrument would stand legal review and opposing challenge."

Keywords: X_ways, Cybersecurity, Forensics, Detection, Cyber space, Examiners

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

Citation: Seth Adjei Gyimah (2022): X-Ways Forensics Platform For Digital Forensics Examiners
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 353-356
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P56

1. INTRODUCTION

Digital forensics has become a recognized profession and research field because of the rapid increase in the use of computers, electronic devices and the rise in cybercrimes. Digital forensics is an act whereby investigative techniques, methods and tools are used to gather evidence from a cyberattack or cybercrime. Due to the importance of evidence provided by a digital forensics examiner, processes and operations like data extraction, storage and analysis should be conducted in robust environments using scientifically proven methods and legally acceptable tools. X-Ways forensics is one the forensic tools on the market for conducting thorough forensic examination.

X-Ways Forensics, the forensic edition of WinHex, is a powerful and affordable integrated computer forensics environment with numerous forensic features, rendering it a powerful disk analysis tool: capturing free space, slack space, inter-partition space, and text, creating a fully detailed drive contents table with all existing and deleted files and directories and even alternate data streams (NTFS), Bates-numbering files, and more.

It also serves as a low-level disk imaging and cloning tool that creates true mirrors (including all slack space) and reads most drive formats and media types, and supports drives and files of virtually unlimited size (even terabytes on NTFS volumes!). X-Ways Forensics can natively interpret and show the directory structure on FAT, NTFS, Ext2/3, Reiser, CDFS, and UDF media and image files. It performs safe recoveries on hard disks, memory card, flash disks, floppy disks, ZIP, JAZ, CDs, DVDs, and more.

1.1 Background to the Study

The goal of digital forensics is to discover, recover and document electronically stored information (ESI) from computers, cell phones, storage devices, and networks for legal purposes. It provides a vital link between today's high-tech crimes and criminal investigations. With software involved in so many aspects of our daily lives, including computers at work and home, smartphones we carry around all day long, wearables, activity trackers, and smartwatches, it's not surprising that digital forensics tools and application software have become so popular over recent years. Statista estimates there will be 7.26 billion mobile devices in use globally by 2022, and 75.44 billion IoT devices will be connected to the internet by 2025. This calls for the development of tools and applications that will help to unravel and solve crime cases. One of such tools is the X-Ways Forensics that this paper seeks to talk about.

The objective in this paper is not to denigrate any forensic application or tool nor neither to place any application or tool in a negative spot. In most cases, a forensic examiner will need more than one forensic application or tool to thoroughly examine and investigate a particular case just like a technician or an engineer will need more than one tool to complete a task. This study will focus on X-Ways Forensics as a primary tool for a forensics examiner and how the application helps in investigation and evidence gathering.

Table 1: Related Literature

Author	Title	Findings
Moses, S. (2017)	Measuring The Robustness of Forensic Tools' Ability to Detect Data Hiding Techniques	Each forensic tool, Autopsy/Sleuth and X-Ways Forensics, was tested against the methodology and provided valuable results. The author revealed that It is logical to conclude that X-Ways can analyze files beyond their extension and header information.
Shavers, B. & Zimmerman, E. (2014)	X-Ways Forensics Practitioner Guide	The authors concluded by stating that though X-Ways Forensics greatly simplifies the forensics workflow, it best serves those who understand the evidence.

Author	Title	Findings
Fleischmann, S., 2012	X-Ways Forensics/WinHex Manual	The author explains X-Ways forensics as an advanced work environment for computer forensic examiners and that it is a powerful and affordable integrated computer forensics environment with numerous forensic features, rendering it a powerful disk analysis tool.

3. RESEARCH GAPS/FINDINGS

X-Ways Forensics is more efficient to use and runs much faster Compared to its competitors. As a German product it is potentially more trustworthy, comes at a fraction of the cost, does not have any ridiculous hardware requirements and does not depend on setting up a complex database. X-Ways Forensics is fully portable and runs off a USB stick on any given Windows system without installation if you want. It also easy to download and install since the executable file is small in size. X-Ways Forensics is based on the WinHex and disk editor and part of an efficient workflow model where computer forensic examiners share data and collaborate with investigators that use X-Ways investigator. X-Ways Forensics requires that the analyst performing the cloning understand the differences between logical and physical media, as well as understand the implications of writing a pattern to suspected bad sectors. A knowledgeable analyst would have no trouble using X-Ways Forensics to clone media in a forensically sound fashion. However, inexperienced analysts who might be used to forensic tools that require less knowledge from the user might have trouble.

4. CONCLUSION

X-Ways Forensics is the flagship product of X-Ways and provides integrated computer forensic software for forensic investigators in governments, research, and industry. Law enforcement agencies rely heavily on digital evidence to build criminal cases against perpetrators and therefore there be should credibility and integrity surrounding the activities and processes used to collect, gather and store evidence. This is where X-Ways Forensics comes in to become the primary and most important investigative forensic software for forensic examiners. Jeffrey R. Gross, President of Computer Forensic Associates, explained the importance of X-Ways Forensics succinctly by stating that “Version 11.1 is great.

You continue to improve upon an already exemplary product and maintain excellent user support. I wish other software producers were in your league. I operate a computer forensic/electronic evidence business and use your product in all my cases almost without exception as a standard first line examination tool. The integration with Windows Explorer enables me to open many files quickly and conveniently under Winhex to quickly assess what I have. A great, reliable and bug free product.”

5. RECOMMENDATION FOR POLICY AND PRACTICES

To effectively address the numerous investigative scenarios surrounding us, a digital forensic examiner will need different collection of forensic applications. It is important to understand that no one digital forensic tool is all-inclusive; therefore, having multiple tools on hand is the best way to gather and present credible evidence. Many of the tools may have overlapping functions, but each application will have unique strengths that add value to an overall investigative process. Having multiple tools on hand that perform similar functions allows processes and methods to be validated. The unique strength of each tool applied to a given problem will allow for a diverse and thorough investigation to take place.

6. DIRECTION FOR FUTURE WORKS

Cybercrimes are getting more complex and complicated and for that matter X-Ways Forensics has to be updated with modern features and functions in order to stay relevant and still become useful to the digital forensic examiner. Its operating system compatibility should be improved to include android and IOS environments. Finally, the application producers should consider hosting it online to avoid the rigorous task of downloading the executable file to install before setting it up before usage. Hosting the application online will make it easily accessible and much more secured to be used by digital forensic analysts.

REFERENCES

1. Moses, S. (2017). Measuring The Robustness of Forensic Tools' Ability to Detect Data Hiding Techniques. 2017 BYU ScholarsArchive
2. Abulaish, M. & Hardar, N. (2018). Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking.
3. Shavers, B. & Zimmerman, E. (2014). X-Ways Forensics Practitioner Guide. Library of Congress Cataloging-in-Publication Data.
4. Fleischmann, S., 2012. X-Ways Forensics/WinHex Manual. Retrieved May 06, 2022, from X-Ways Forensics Computer Forensics Integrated Software: http://www.x-ways.net/winhex/manual.pdf.
5. Abdullahi, A. (2022). Top Digital and Computer Forensics Tools & Software 2022. https://www.itbusinessedge.com/security/digital-forensic-tools/