Academic Journal of Research and Scientific Publishing | Vol 3 | Issue 35
Publication Date: 5-3-2022 ISSN: 2706-6495

The Digital Forensic Tools Accuracy and Specifications

By: Jasir Adel Altheyabi

Master's in Cyber Security, Cyber Security Department, College of Computer and Information Science, Majmaah University, Kingdom of Saudi Arabia

Email: Eng.Jasir@Gmail.com

Abstract:

The research aims to provide an overview of computer forensics, the history of computer forensics tools, and the accuracy and specifications of these tools. With the great and accelerating technological development, the reliance on the Internet has become greater and stronger than before. The world has become dependent on technology in all production and economic operations. And we talked in the second axis of the search for The Computer Forensic Legal Requirement, and Presentation of the tools used in the criminal investigation and an explanation of each tool.

The digital forensic investigation tools that we will explain in this research are FTK. Forensic Toolkit, Prodiscovery, Autopsy, p2commander, OSForensics.

We conclude that digital investigation tools have outstanding performance on different mediums. It has high accuracy and efficiency in digital investigation, and no single tool is superior to some other tools in all media. With more than one tool on a range of devices, it improves the investigation and testimony capabilities of examinees during exploration.

Keywords: Digital Forensic Tools, Digital Forensic Tools Accuracy, Digital Forensic Tools Specifications

1.1 Introduction

Investigation in its general concept means investigation and scrutiny in the search for something in order to ascertain its existence, or seeking to reveal the ambiguity of a particular fact, and for this should use specific methods and means guaranteed by law to conduct the investigation, and the concept of investigation has long become a tangible reality of a science called forensic science It is a science that specializes in investigating and researching crimes committed by various members of society (Al-Zanoun, 2001).

Digital forensics is the process of investigating crimes committed using any type of computing device such as computers, servers, laptops, mobile phones, tablets, digital camera, networking devices, Internet of Things (IoT) devices or any type of data storage device.

The digital forensic investigation aims to retrieve computer files and all materials related to the investigation, analyze and save them in a way that helps the investigation authorities to present them as evidence in a court of law and in a manner befitting the judicial system, knowing the main motive behind the crime, the identity of the main offender, the nature and history of the relationship between the offender and the victim, completing and designing procedures at the scene suspected crime, which helps ensure that digital evidence obtained is not corrupted. Data acquisition and copying: Recover deleted files, deleted and encrypted sections of digital media for evidence extraction and validation.

Quickly identify evidence, and allow assessment of the potential impact of malicious activity on the victim, produce a computer forensic report and provide a complete report on the investigation process from start to finish, save all evidence in multiple copies and in secret storage spaces.

1.2. Objectives:

The current research aims to:

- Provide an overview of computer forensics
- History of computer forensics
- Legal requirements for computer forensics
- Presenting the most important digital forensic tools used in computer forensics.

1.3. An Overview of Computer Forensics

Computer forensics is also a scientific process that uses technology to review media and digital devices. Computer forensic practitioners must develop and establish a hypothesis regarding an incident or series of events. Which could be entered as a guide for courts or inquiries.

To prove or refute a hypothesis. The investigator must identify and extract evidence. This evidence includes among other things: documents. internet activity. User and computer activity. In many cases. This guide may are deleted or obfuscated (computer forensic services. No date). So on locate and extract computer evidence. Investigators may use a forensic tool or computer tools.

It is important that when identifying. Extracting. Archiving. And presenting evidence. The tactic must be repeatable. Which the evidence will accommodates relevant laws and acts. The simplest way within which hypotheses are proven is by using digital forensic tools that extract data that the computer forensic investigator interprets. Therefore it's essential that investigators be able to trust the knowledge provided by the tools. The simplest way to verify the knowledge provided by the tools is to use a special tool.

1.4. History of Computer Forensics Tools

Modern computer forensic techniques have their roots in data recovery techniques. Which have been employed in a manner to make the recovered data admissible (Mercuri, 2010). Purpose designed computer forensic tools were originally proprietary tools developed by Guidance Software and Access Data for and available to law enforcement agencies only.

In 1999. The Coroners Toolkit (TCT). an open source digital forensic tool for UNIX systems was presented. TCT was extended to include support for FAT and NTFS le systems by a team lead by Brian Carrier who later developed one of the leading forensic tools; The Sleuth Kit (TSK) (Carrier, 2005).

2. Literature Review

2.1 Computer Forensics and Computer Forensic Tools

Computer forensics is approximately 49 years old. Modern computer forensics strategies have been in the beginning developed out of a want to recover statistics that were by accident erased. These recovery strategies have been first of all used by laptop experts in helping law. Forensic tools persevered to be advanced in response to specific threats. And not because of coordinated e orts. Computers were seemed as inconsequential factors in crime scenes and therefore their fee to deliver essential evidence changed into underestimated. However as the range of cybercrimes increased. The cost of virtual proof became more apparent and appreciated. Ensuing in computers being recognized as assets of vital proof (Storer et al. 2019). As a result. Forensic investigators and researchers identified the requirement for the improvement and standardization of a computer forensic framework. A not unusual virtual forensic format (Digital Forensic Research Workshop. N.D.) and research agenda. Further-more a set of fundamental requirements to which computer forensic tools have to adhere had been identified. To fulfil these requirements. Tools have to be relatively smooth to use. Comprehensively discover all evidence. Be correct and deterministic. And their accuracy ought to be verifiable (malwarehelp.org, 2014).

2.2 Objective of Computer Forensics

The overarching objective of pc forensics is to render binary statistics as electronic evidence. And to collect. Analyze. Preserve and gift that electronic evidence in a manner that makes it admissible in a court docket of law. Inner disciplinary enquiries or different tribunals. Evidence is but no longer restricted to whole files that are intact on digital media. However includes remnants of user sports and deleted facts It is of paramount significance that the authenticity and integrity of the evidence extracted and presented with the aid of computer forensic gear is maintained. Authenticity of evidence is satisfied via demonstrating that the evidence has no longer been altered. One manner of ensuring authenticity is by maintaining the chain of custody by using retaining thorough documentation. The documentation have to le have to every movement and or system carried out in collecting.

Reading and exporting data. Records of conditions beneath which proof is stored in addition to whom the custodians and handlers of the proof were are vital records that need to form part of this documentation. Reliability of proof is installed by way of demonstrating that results can be repeated or tested Integrity of evidence in the digital realm may be tested by the usage of cyclical redundancy checks (CRC) and cryptographic hashes to make certain that copied proof is exactly similar to the original. Preserving the chain of custody is another a part of preserving integrity of proof (Carrier, 2014).

2.3. The Computer Forensic Legal Requirement

From legal aspects. Computer forensic investigators need to make sure that the method that they observe is technically indeniable and able to withstand legal scrutiny. Furthermore. The evidence provided to court wishes to be accurate. Validation of findings through the usage of different pc forensic gear is one manner of making peace of mind that evidence is accurate. Repeating the investigative system with a different tool also lets in an investigator to validate the procedure. Another benefit of validation is that investigators are capable of verify that they did not by accident introduce new evidence or omit existing proof. (Watney, 2009).

Once evidence has been submitted to court docket. It's far in all likelihood that the investigator will be called upon to testify to that evidence. The purpose for this is that proof has little or no evidentiary price unless observed by testimony. Investigators need to stay aware that presiding officers in court proceedings aren't virtual specialists and depend upon the testimony of expert witnesses to give an explanation for their findings. The integrity of a computer generated report is taken into consideration to be intact if it can be shown that the facts it contains is complete and has remained unaltered Nist.

2.4. Digital Forensic Tools

2.4.1. FTK. Forensic Toolkit

In order to create photos. Access Data evolved a unfastened proprietary tool known as FTK Imager. FTK Imager is capable of make pix of each static resources which include di cult drives or reminiscence sticks as well as of unstable resources including reminiscence from RAM physical reminiscence and from video or network cards (Business Wire, 2013).

Using FTK Imager. Practitioners are able to preview or picture quite a few le systems inclusive of FAT. NTFS. EXT. CD. DVD and AFF. FTK Imager is capable of create images in .001,. S01, .E01, .AFF, .ISO and Access Datas proprietary. AD1 format. Previewing media is beneficial in appearing triage as investigators are capable of pick whether or not or no longer they want to image a digital source and if so. Whether or not they need to photo-graph all contents on the supply or most effective specific content material. Furthermore. Investigators are capable of make custom content pics. Which consist of selected content from a digital supply added to one photograph. All photographs may be verified the use of MD5 and SHA1 or each hash calculations. Investigators are capable of use Access Data encryption to encrypt images.

Investigators are capable of use FTK Imager to mount screen shots as drives on a Windows machine. Mounting of photographs permits investigators to view files in photos of their native packages and to copy files from the image. Image mounting also enables investigators to run anti-virus software program on mounted pictures. Thereby gaining advance warning of capacity threats and testing allegations of virus or malware.

2.4.2. Prodiscovery

Effective computer security device that enables regulation enforcement experts to locate all the information on a laptop disk while protective proof and developing evidentiary excellent reviews to be used in criminal proceedings.

ProDiscover is a disk forensics machine which gives a bunch of capabilities to capture and analyses disks. The product supports a wide sort of Windows. Linux and Mac record systems. ProDiscover ensures that both the taking pictures and analysis techniques are completed by way of applying forensically sound methods. The resulting reviews meet evidentiary pleasant requirements.

2.4.3. Autopsy

Autopsy provides a graphical consumer interface that may be used in con-junction with TSK. E01 and dd photos may be analyzed the use of Autopsy that may run on Windows.

Linux and Mas OSX platforms. Aside from its analysis function. Autopsy is ready to perform keyword searches and generate reports (Carrier, 2014).

2.4.4. p2commander

P2 Commander is a court docket proven. Laptop forensic answer for examiners who want affordable. Reliable virtual evaluation for computer investigations. Built to process huge volumes of statistics in a quick and green manner. P2 Commander is understood for its advanced e-mail and chat log evaluation.

2.4.5. OSForensics

OSForensics from PassMark Software is a virtual computer forensic application which lets you extract and examine digital information evidence correctly and with ease. It discovers. Identifies and manages ie uncovers the entirety hidden internal your computer systems and digital garage devices.

OSForensics is a self-capable and standalone toolkit which has almost all the virtual forensics abilities including Data acquisition. Extraction. Analysis. Email analysis. Facts imaging. Image restoration and plenty more.

In this article. We will cover all of the major talents of these forensics tools for virtual forensics investigations.

3. Acknowledgements

To Doctor Talal Alharbi. My supervisor who was always available to guide and encourage me. First Majmaah University support. Resources and time o to complete my studies. Appreciation is also expressed to my colleagues for their encouragement and support.

4. Conclusions:

We conclude that digital investigation tools have outstanding performance on different mediums. It has high accuracy and efficiency in digital investigation, and no single tool is superior to some other tools in all media. With more than one tool on a range of devices, it improves the investigation and testimony capabilities of examinees. During exploration.

The seting of fundamental computer forensic tools requirements adhere had been identified. The Tools have to be relatively smooth to use. Comprehensively discover all evidence. Be correct and deterministic. And their accuracy ought to be verifiable.

5. References:

Al-Zanoun, Salim (2001) Criminal Investigation: General Principles of Criminal Investigation, The Arab Institute for Studies and Publishing, Beirut, Lebanon.

Storer T, Glisson W, Buchanan-Wollaston, J. A (2019). Comparison of Forensic Toolkits and Mass Market Data Recovery Applications. In: International Conference on Digital Forensics.

Carrier, B. (2005). File System Forensic Analysis. Addison Wesley.

Carrier, B. (2014). Autopsy Analysis Features. http://www.sleuthkit.org/ autopsy/features.php.

MalwareHelp, (2014). Free Forensic Software Tools. http://www.malwarehelp. org/forensic$_t$ools:html.

Mercuri, R. (2010). Criminal Defense Challenges in Computer Forensics. Pages 122138 of: Goel, S. (ed), Institute for Computer Science, Social- Informatics and Telecommunications Engineering.

Watney, M. (2009). Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position. Journal of Information, Law Technology.

(Watney, 2009)

Business Wire, (2013). Access Data Introduces Forensic Toolkit (FTK).

Doi: https://doi.org/10.52132/Ajrsp.e.2022.35.3