International Journal on Engineering Technologies and Informatics

Digital Forensics Tools

Review Article

Volume 3 Issue 3- 2022

Author Details

Asia Othman Aljahdali, Joud Abdulfattah, Thana Aljohani, Remaz Alawaji, and Suha Almuhanna*

College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

*Corresponding author

Asia Othman Aljahdali, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

Article History

Received: October 26, 2022 Accepted: : October 27, 2022 Published: October 28, 2022

Abstract

The increase in digital crime has created an urgent need for digital forensics. The evidence must rely on information collected to prove it. Digital forensic tools would help investigators discover this information. On the contrary, some computer forensic tools suffer from the unreliability of the assembly and verification of the required response. This study presents an overview of computer forensics tools and their evolution, and the criteria by which we can choose the appropriate tool for a case to extract the important artifact that enables the investigator to extract reliable evidence. Additionally, the paper studies the most popular forensic tools and compares them in terms of their features and functionality to help in choosing the appropriate tool for a particular case to discover more reliable information and evidence.

Keywords: Computer forensics, Digital evidence, Artifact, Forensic tools, Metadata

Introduction

The increase in the use of electronic ways of performing things has revolutionized life at large. People are using digital tools to communicate, send data, and even perform transactions. This has consequently affected the way data is stored and generated, with the volume of data skyrocketing every day. Data storage and analysis have also improved to accommodate the large size of data. But, what about people who want to exploit the data for malicious purposes? With data readily available, it has created loopholes in which the data is always compromised; in fact, the use of digital tools has also facilitated an easier method of attack, where physical presence at the crime scene is not required. This has increased the number of crime cases perpetrated using a digital device. Because of the complexities and uncertainties involved in resolving cybercrime, digital forensics is an important requirement [1]. The digital revolution has helped in dealing with traditional sophistication that was prevalent. This has eased people's interaction. This has opened the way for crime to be perpetrated using those tools. Digital crimes are hard to prevent, detect, and revert, leaving many communication and transaction channels at the mercy of the crime perpetrator. Digital forensics came into being in order to protect people and businesses from these criminals. Most of these attacks leave a track that is hard to detect. Digital forensic is the preservation, identification, extraction, and documentation of the evidence collected during the analysis so that it can be used by the court of law [1].

This paper discusses the evolution of digital forensics, compares four different forensic tools, and provides recommendations for improving digital forensic tools and their functions. These guidelines would seek to fix some of the shortcomings of previous tools. Section 1 discusses forensic tools' evolution, validation, and what are the criteria for choosing the right tool for your case. Section 2 presents tools for editing and extracting internal file metadata and how they work, as well as the main features and limitations of these tools. In sections 3, 4, and 5, we study the most popular forensic tools, which are the Rediscover, Forensic Toolkit (FTK), and Kroll Artifact Parser and Extractor (KAPE) tools. We present their main features, and how they work, respectively. As for the sixth section, we discuss the limitations of forensic tools, and then we compare the previously discussed tools based on their functionalities and features. At the end of the paper, we present a conclusion and recommendations. This research aims to conduct a literature review of computer forensic tools and their evolution to determine optimum criteria for selecting the tool in proportion to the situation to extract reliable evidence.

Computer Forensic Involvements

Computer forensics (CF) tools are currently utilized every day by

investigators and analysts, which become an important part of numerous investigations. CF tools allow investigators to capture, store, and analyze data to create evidence for legal procedures [2].

The Evolution of Computer Forensics Tools

There are several synonyms and meanings for the term "computer forensics." This began with early law enforcement officers in the late 1980s who used computer forensics to refer to the search of individual devices for digital proof of the crime [3]. Others have argued that forensic computing is a more accurate term, particularly as digital evidence is increasingly being collected from artifacts not generally thought of as computers (such as digital cameras). Notwithstanding this, we use the general term "computer forensics" here to refer to both the workstation and the forensic disciplines based on electronics [3].

The Criteria to Choose the Right Tool for your Case

Often, the cycle of prejudice in choosing the right thing is complicated with major implications, such as selecting the correct forensic tool. Such a case requires a systematic, organized methodology before choosing the appropriate investigative method, and one of those methods is "decision analysis" [4].

Forensics experts had previously selected the tools based on heuristics (based on their experience) about the performance of the forensic tools using probability theory. Most examiners pick the instruments of forensics without adopting a structured system of efficiency and significance for quantification. Therefore, they behaved in confusion. If you have a multi-criteria decision analysis, a decision-maker will analyse and coordinate several typically opposing decisions and criteria, also optimizing total gain/output during the decision making [4].

Following the acquisition of the contents of the hard disk drive (HDD) image, files are analyzed to show evidence that either supports or undermines a hypothesis or for signs of alteration (to hide data). During the study, an investigator typically recovers evidence material using a variety of different methods and tools, mostly starting with the recovery of deleted content. Examiners use specialized software to help in displaying and retrieving the data. The type of recovered data varies depending on the investigation. The data may be retrieved from available disk space, deleted (unallocated) space, or from cache files within the operating system [5]. In addition, as discussed in [6], a digital investigator must be aware of some features and conditions that must be available in the forensic tool he selects for his case.

From a legal point of view, non-repudiation is one of the most important criteria of digital evidence presented in court, as well as the verifiability of that evidence. Furthermore, the digital evidence and the procedure of obtaining that evidence must be repeatable in case a subsequent court action is required.

From a management point of view, a forensic tool should be available to the investigation firm at a fair cost from a reliable vendor who provides a good support and training services. From a technical point of view, the precision of the information and evidence obtained by a tool for a given forensic investigation is the most important matter. Also, a forensic tool should be able to produce log files to track all activities carried out by the forensic investigator. This feature allows auditors to check the procedure and ensure the integrity of the evidence produced. In addition, the presentation and reporting functionalities of a forensic tool provide a helpful way to communicate the investigation results to recipients with no technical background. Other technical features that a forensic tool should include are usability, reliability, and efficiency.

Validation of Digital Forensic Tool

The domain of digital forensics relies heavily on the tools to collect and examine types of digital evidence. Analysing digital devices would not be feasible without such tools. Moreover, tools are available now using various techniques and approaches. While tool errors raise one question, identifying the limitations of a tool also presents an investigative challenge that leads to the likelihood of professional user error and, ultimately, less liability. Software bugs have always been a major problem that would be detected and patched later in the ongoing development of computer software, but when it comes to forensic software, a small software bug may lead to important evidence being missed or interpreted and analysed incorrectly, which would be very misleading to the investigation trail. Therefore, the accountability of such software is always questionable. This illustrates that professionals must validate the precision of the techniques they use throughout the process of digital investigation [7,8].

As defined in [8], "validation is the confirmation by examination and the provision of objective evidence that a tool, technique, or procedure functions correctly and as intended." Furthermore, since misleading evidence will not only affect the parties involved in a criminal case but also affect the professionals who provide and analyse that evidence, in the process of validating digital forensic tools, professionals cannot consider the word of the software developer without further confirmation [7,8].

Validation techniques can be classified into two categories based on the approaches and methodologies used:

- Tool-oriented validation approach. An example of this approach is when the validation work is done by the software developers, generally by conducting a series of tests for each function of the software and analysing the test results and findings objectively. The problem with these tests is that they are usually not documented and that they might be biased. The shortcoming of the tool-oriented validation approach is that it deals with forensic software as one box, so if a particular function on a software does not pass the test, this approach will consider the entire software invalid. Moreover, this approach is considered very complex and not cost-effective [8].

- Functionality-oriented validation approach. In this approach, the processes of digital investigation are distinguished, and in each process, different essential tasks are identified. After that, each task is assigned to one or more functionalities like keyword finding, disk imaging, etc. Then, a set of requirements is assigned for each function, and candidate software functions are tested against these requirements. The advantage of this approach is that it provides a more effective and flexible validation procedure which focuses clearly on the assurance of a certain function regardless of the other functions available in a software package [8].

The distinction between a digital forensic tool error, a tool limitation, and a tool user error must be considered first. While it can appear logically clear, it is a difficult task to identify the three in practice. A tool error occurs when an application or software package misinterprets or misrepresents data that is the subject of its investigation. Tool errors can come in the form of false positives where evidence is provided by the forensic tool, but it does not actually exist, or they can come in the form of false negatives where evidence is not detected although it exists [7,9]. A tool limitation defines the confines within which an application or software package can be expected to reliably operate. [7]. Tool limitation determines the limits of the capability of a tool [7]. A tool user error defines the use of a process, procedure, or tool for a purpose or in a way that it was not designed to be utilized. It is worth noting that ambiguity in tool limitation documentation can sometimes lead to user error [7,9]. Finally, the process of validating and testing forensic tools normally goes through common steps. First, a researcher should obtain the tool to validate and review its manual and documentation. Then, he should prepare test cases and associated test policies. After that, he will run test cases and provide test reports to a consulting committee for evaluation. Then, test reports should be sent to the tool vendor, and the legal authorities will publish the validation results to interested parties [10].

Tools for Editing and Extracting Internal File Metadata

Metadata is data about data. For example, the metadata of a Word document includes the author's name and the dates the document was created or modified. The metadata is embedded into the file itself, and it contains information that an investigator might find useful. For example, digital camera images may contain an extended file information (EXIF)-Exchangeable image file format-header that saves information about the camera that took the image. The EXIF format was created by the Electronic Industry Development Association of Japan and is referenced in ISO (International Organization for Standardization 12234-1) as the preferred image format for digital cameras [11].

For example, metadata may enable a forensic investigator to gather vital evidence such as whether or not a photograph was taken, what camera was used to capture the image, who took the photograph, and where it was taken. The EXIF metadata format also allows digital camera designers to provide details such as camera and model configuration, camera settings, date, publisher, copyright, and other information in the image file so that the owner can keep a permanent record of this info together with the image [12]. All of these are key points to assist investigators in analysing the evidence and discovering the facts about the electronic issues. Photo editing technology is rapidly developing. Generating manipulated images has become so simple that photographs can no longer be trusted. Working on the identification of image forgeries has thus turned out to be a critical activity nowadays.

There are several ways of image editing. The three principal ways of interfering are adding, removing, and altering. Because of its simplicity, image area copying, and pasting have become one of the most popular manipulation techniques [13]. Typically, if the image is copied and pasted in an area, it may be blurred, or the degree of brightness and exposure can be changed. And alternative platforms to hide data or to prevent some of the privacy and ethical problems that impact the systems that are most used, including software packages like Exif Tool and Analog Exif.

EXIF Tool-Exchangeable image file format

The Exif tool is an open source for reading and modifying Exif metadata tags associated with audio, video, documents, images, and media files. The Exif tool is an executable program (command line application) and libraries. To have a multitude of metadata elements for analysis, the stand-alone version can be executed against any single file [14]. Understanding that this information may be spoofed without verification, it is extremely important in forensic examinations. The Exif Tool could be used to adjust the metadata values when analysing the metadata for an image or other file type. Illegal values can also be written to metadata records using Exif Tool. Improving the personal experience of what to expect in places that are important to investigations will help signal the presence of criminal values in those fields to begin with [14].

Analog EXIF

It is a free, open-source program that can be used to edit metadata for the scanned movies and digital images collected by digital still cameras (DSC). It can also modify any JPG and TIFF image metadata area for editing or deleting embedded metadata until they are shared on digital files. Moreover, it allows users to access and edit the embedded information in different types of files; doing so will alter or wipe out information that may be potentially useful when arranging the content or attempting to look for it later [15].

The developers of Analog EXIF specify in the documentation many features. One of these is that a single metadata has more than one specific tag. This tool has a library for storing the metadata properties of the film cameras, and it includes a custom XMP schema (Extensible Metadata Platform) for properties of the film camera, e.g., film name, exposure number, etc., and enables extra user defined XMP schema. Also, it stores metadata values in the comments of the image; this is for easy viewing in Explorer and for most of the basic viewers. Additionally, it allows single and multiple batch operations, such as copying metadata from another file, auto-filling exposure numbers. It is customizable and has a flexible set of supported metadata tags. It also provides internationalization and supports multi-platform editions (Win32 and Mac) and Google Maps. Figure 1 shows the main interface of the Analog EXIF.

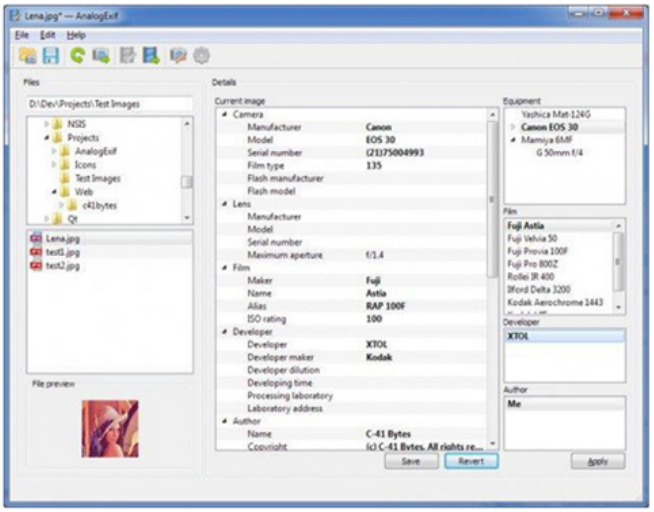

Figure 1: Main interface (Win7).

ProDiscover

ProDiscover is basic in general. It is a strong digital forensic investigation and examination tool utilized for the assessment of hard disk security, which permits you to image, break down, and report on evidence that is found on a drive to create an evidence report for legal procedures. When you insert a forensic image, you can view the information by content or by looking at the clusters that hold the data and searching for a word anywhere on the disk [16]. Pro Discover helps investigators to recover the deleted files as well. It assists in gathering event time zone information, drive data, and internet activity [17]. ProDiscover has strong search capacities for capturing unique data, file names, document types, information designs, and date ranges. In addition, it allows the investigator to extract the data and show when the file was accessed last and if any modification has been made to it [18].

Pro Discover Forensic is a useful digital forensic investigation and examination tool to ensure the confidentiality and integrity of the system, and if it has been compromised, it allows investigators to capture and examine a full disk. It provides useful evidence reports that are used in legitimate proceedings. It supports a wide assortment of Windows, including FAT12, FAT32, and all NTFS file systems; Linux, Mac, and supports VMware. When Pro Discover is incorporated with a search engine, it can be a keyword or full text and hash comparison, all together giving a simple-to-utilize and incredible toolbox to forensic investigators [19]. Some features of Pro Discover forensics provided to investigators include maintaining the data integrity of evidence files, which includes automatically recording MD5, SHA1, and SHA256 hashes of files. Also, Pro Discover maintains the original evidence to be safe by creating a bit-stream copy of the disk [19]. Pro Discover is a forensics tool apparatus that empowers PC experts to find all the information on a PC storage medium while securing evidence and making quality reports [20].

Pro Discover Incident Response helps in gathering information as evidence to prove if the system has been compromised or not. Some features of Pro Discover incident response include, firstly, examining live systems forensically remotely via the network. In other words, it supports the remote acquisition and reads the suspect disk bit by bit, which helps to investigate and examine the disk precisely [19]. Also, it provides features for computer forensics with tools for complete incident response. It features all the essential IT forensic capacities, including a capacity to discover hidden information, hash-keeping, file metadata data, and all can be done via network [21]. All the data is protected with 256-bit AES encryption, which is transferred over the network. To investigate an incident, Pro Discover allows capturing data links, such as what ports are open with IP, logging users, and ARP cache [19].

Pro Discover Pro acts as a storehouse for Pro Discover Forensics and Pro Discover Incident Response. Data recuperated is saved in a secure way and put on a web platform. Some of its features include supporting Boolean, Date, and heuristic searches to discover file names and content across all the documents that were captured from a disk. It also creates and manages content reports [19]. Figure 2 shows the main interface of Pro Discover, which has many options that help the investigators capture the disk.

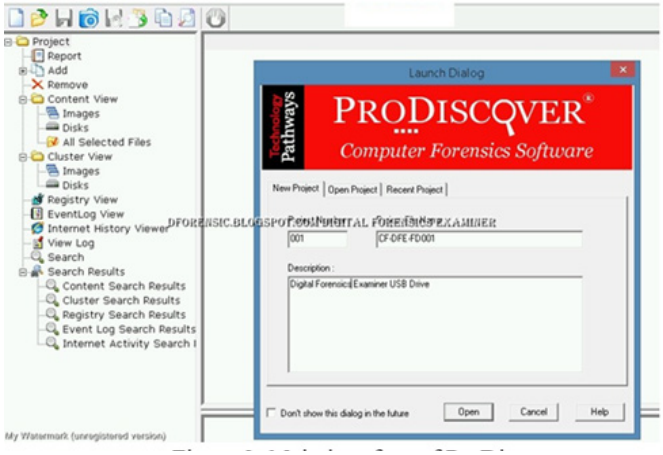

Figure 2: Main interface of Pro Discover.

Forensic Tool Kit (FTK)

FTK is a digital forensic software developed by Access Data. The company provides different digital forensic software for law enforcement and government agencies. FTK is among the best software to be developed for computer forensic services. The software works by scanning the computer hard disk for suspicious data, including deleted emails. The high operation speed makes the software palpable for resolving crimes involving large data sets. The high speed is a result of its operation technique of indexing data upfront. High speed and reliability have made FTK a critical tool for digital investigation. The tool has different features that enable it to perform the task successfully [22].

Figure 3 below shows the final step to cleaning the disk after adding the evidence because FTK was not able to find any usable data.

FTK Imager and Explicit Image Detection (EID)

These are important tools in saving data for future use. The FTK imager allows disk imaging where an image of a hard disk is saved as a file or in segments. The imager uses MD5 hash value technology, which allows the image to be saved in different formats. The technique also enables validating the integrity of the data. The EID helps detect images and can be used for detecting pornographic image materials [23].

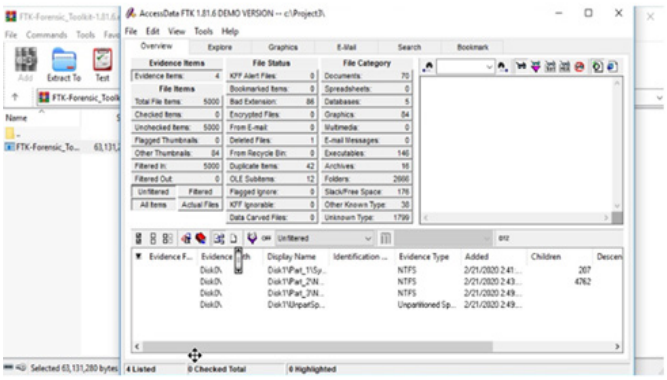

Figure 3: The Access Data FTK Window.

The features that are provided by FTK are as follows

Database-driven, FTK has successfully deployed its services where its operations are database-driven. This allows the software to run without the crushing caused by memory-based data access. The feature also allows the data to be centrally placed, so there is no need for multiple datasets.

Cerberus add-on, FTK has a high capability for malware detection, analysis, and triage. Cerberus also offers security services, making FTK more reliable [23].

Decryption and encryption, one of the best features of FTK is its data encryption techniques. FTK has the capability of decrypting PDFs, making it an effective way to resolve documents. The effectiveness of the decryption services makes the use of FTK more reasonable and enables concealing data while stealing access to encrypted data [23].

As a reporting tool, FTK is being used more often as more cases require digital forensics to resolve. Analysing the acquired data is not enough as it may be hard to deduce a good decision from the data. FTK resolves this problem with a good reporting technique. The reporting capability helps present analysed data in a way that good decisions and follow-up can be done [23]. FTK produces a case log file, which makes it easy to track the series of events happening. Moreover, the tool has a friendly user interface, which makes using it easy and understandable. Also, the database-driven feature makes it too reliable. It is hard for the system to crash during an operation. Furthermore, the upfront indexing makes the tool fast. In addition, the tool scanning operations are extremely fast, allowing the analysis of large sets of data [22].

Kroll Artifact Parser and Extractor (KAPE)

First introduced in 2018, KAPE is essentially a triage system that addresses a computer or storage medium, identifies the most important objects forensically, based on investigator needs, and parses them in a few minutes. Because of its speed, KAPE helps investigators find and organize their cases against the more important systems. Furthermore, KAPE may be used before the start of the imaging process to identify the most sensitive artifacts. While the imagery is complete, the data produced by KAPE can be checked for leads, timelines for development, etc [24]. KAPE utilizes the targets and module structure to do its job. KAPE comes with a set of default targets and modules most used in forensic examinations [24,25].

KAPE mainly has two basic functions: a) File collection (KAPE Targets): KAPE operates at the highest level by connecting file masks to a queue. Then, this queue will be used to locate and copy files from an origin location. A second run bypasses the lock for files that are protected by the operating system. KAPE will make a copy at the end of the cycle and retain metadata regarding all available files in a given directory from an origin location [24,25]. b) Process collected files

(KAPE Modules): This is an optional stage. A KAPE module is a set of specifications and properties used to run programs or algorithms. At this processing point, KAPE must run one or more algorithms against the gathered data. That too works by either targeting different file names or folders. Different algorithms run against the data, and the program output is then saved in folders named after a group, such as evidence of execution, browser history, or account usage [24,25]. Figure 4 below shows the graphical user interface of KAPE with different Target and Module options.

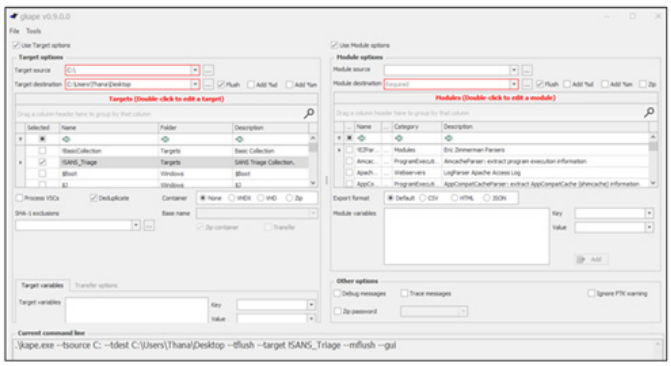

Figure 4: Graphical User Interface of KAPE.

KAPE is a powerful free software. One of the most important advantages of KAPE is that it is fast and flexible since its functionality can be extended easily. KAPE has very good logging capabilities [24], and it can be used on a live system or on a mounted disk image. Moreover, it can use F-Response to work on a remote collection [24,26]. In addition, KAPE can be used to automate the process of creating timelines [26]. Another interesting feature of KAPE is output grouping based on evidence type, which allows investigators to find the evidence they are looking for easily, regardless of the source of this evidence or the experience of the investigator (time-saving) [24,25]. Also, KAPE can work in real time or batch operations and provides both a command line and a graphical user interface [25].

KAPE's graphical user interface contains a Target and Module configuration editor, including automated configuration file validation. This allows you to start with an existing template, make some changes, and then add a new name to the modified configuration [27].

Discussion

In this section, we will discuss the tools previously mentioned and compare them, empathizing with their limitations. The Exif Tool includes hundreds of command modifications that can be used to view, create, modify, or remove elements within the contents of the metadata. Not all these modifiers of commands are especially useful; others are not available either. When new versions of the metadata standards and even the tool itself have evolved over time, some of the modifier commands have ceased to be relevant and either no longer work or have no elements of content to impact [14].

Exif tool and Analog Exif define file formats and are also specialized in extracting essential properties from file formats. They do not conduct a validation of file formats. The main purpose of these tools is to extract and alter metadata from the EXIF file format, which is specialized in storing digital camera and scanner output metadata. But Exif tool also works with a vast variety of file formats in addition to the EXIF file format and includes most of the popular file formats that are widely used to store information. It is also used for defining and extracting significant properties of various file formats in the sense of digital preservation [28].

Por Discover compares the hash value that has metadata with the hash value of an image file when loaded in Por Discover, so if the hashes don't match, it notifies you that the acquisition is invalid and can't be viewed or considered as reliable evidence. Some of the format image files don't contain metadata, such as (.dd extension), so it must be validated manually to ensure the integrity of the data [29].

FTK has the capability to connect to databases and has a central repository of information to prevent the software from constant crushing. The software also supports analysing data in different formats and from different sources [24]. KAPE is considered a relatively new forensic tool [22], so there is a lack of objective reviews and training resources. There are almost no academic articles reviewing and validating KAPE. Exif Tool won't rewrite a file if it detects a serious file format problem. Exif Tool and Analog Exif have been tested with a wide variety of different images, but because they can't be checked with every known form of the image, some files might be corrupted; thus, investigators need to make sure to maintain file backups. While Exif Tool and Analog Exif do some validation of the written content, it is still possible to write illegitimate values that can trigger problems when reading the images with other tools. Also, you must validate each detail of the data every time. Exif Tool is not guaranteed to fully erase metadata from a file while attempting to uninstall all metadata. For JPEG photos, all application segments (except for Adobe APP14, which is not removed by default), and trailers are removed, which effectively removes all metadata, but the results are less complete in other formats [30]. Pro Dicover requires investigators to install the agent (as a server applet) on the target system and kernel-mode driver to access physical memory in some versions of Windows [31]. Furthermore, it is unable to search for or locate Unicode text data [29].

FTK has a file limit that does not support many files, exceeding 2 million files. This may inhibit its usage in cases where many different operations are performed. Also, the tool does not have a status bar. It is hard to know the progress of an operation. This is heightened by the fact that it has no timeline in its sorting data columns. Making progress is thus hard. Furthermore, FTK does not support scripting features and it does not have multi-tasking capabilities.

KAPE has some limitations on the recursive functionality of "find folders". In addition, KAPE has no authentication mechanism to provide more security for the ongoing investigation findings [24]. A comparison between the previously discussed tools based on their functionalities and features is given in Table 1, summarizing, and highlighting the most important functionalities and features.

All the forensic tools mentioned here are free, flexible, and work with most operating systems. Exif Tool is open source. The extraction and adjustment processes are quite clear, as they deal with metadata. Furthermore, all the tools provide GUI processes, but only Exif Tool and KAPE come with command line processes. In addition, all tools provide us with a full report as evidence. FTK and KAPE are both adaptable, with the ability to easily expand and extend their functionalities. In Pro Discover, FTK encrypts the data and uses hashing to provide the integrity, including KAPE. Also, it can search by keyword anywhere. KAPE has very good logging capabilities, while other tools do not. KAPE and FTK provide batch mode, which works by placing one or more commands to be run automatically at a specific time. KAPE, Analog EXIF, and Exif Tool handling with a script for the language also classify the outputs as specific groups. Pro Discover, FTK, and KAPE can do remote functions such as examining live systems forensically remotely via the network. In addition, it can do a full or partition disk image. Pro Discover, FTK, and KAPE can support the virtual machine [32-36].

For a forensic tool, we recommend the presence of functions that verify all the details of the metadata used in Exif Tool and analgesic, and also that automatically backup copies of the files, and that the programs are expanded so that the user can add other functions to edit, delete, or copy the metadata. In addition, we propose that Pro Discover include a feature that allows it to search for any type of data, including Unicode text, and then decode it to ASCII text independently. In the end, we recommend that more research be conducted to apply formal testing to validate KAPE.

Table 1: comparison of computer forensic tools functions.

Functionalities and Features	ExifTool and AnalogExif	ProDicover	FTK	KAPE
Operating system (Mac –windows - linux)	√	√	√	√
Open source	√			
Free	√	√		√
Metadata format	√	√	√	√
Disk image		√	√	√
Disk / partition		√	√	√
Virtual machine		√	√	√
flexibility	√	√	√	√
Extract and Edit	√	√	√	√
Command line processes	√			√
GUI processes	√	√	√	√
Remote functions		√	√	√
Reporting	√	√	√	√
Output grouping	√			√
Log reports				√
Batch operation			√	√
Scripting languages	√			√
expansion			√	√
Hashing		√	√	√
Keyword search		√	√	√
Encryption		√	√	

Conclusion

With the increasing number of cyber-crimes, investigators need to use digital forensic tools to help them find useful evidence. Digital forensic tools aid in determining when, where, and by whom data was accessed, modified, or used for other purposes. We reviewed some of the most famous forensic tools and we discussed and presented their features and limitations. We also compared the tools based on their functionalities and features and provided our recommendations. In addition, we discussed the process of validating and testing forensic tools. Finally, we concluded, that KAPE has more features than others. In other words, KAPE has comprehensive all the features that are in Exif Tool and Analog Exif, Pro Discover, and FTK, as we did in the previous comparison. In contrast, the tools for extracting metadata are many, and the most famous of them are mentioned in the paper. Because of weaknesses, the investigator cannot verify the validity of the results presented. Also, some functions are suspended due to the different versions, which causes problems in the reliability of the evidence. On the other hand, all the tools that we present in our paper also have their own features and weaknesses. Thus, investigators would choose the appropriate tool depending on the case and their knowledge of these features and limitations.

References

1. Arshad H, Jantan A, Isaac AO (2018) Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence.
2. Garfinkel Simson L (2010) Digital forensics research: The next 10 years. digital investigation 7S64-S73.
3. Yasinsac, Alec (2003) Computer forensics education. IEEE Security & Privacy 1.4: 15-23.
4. Saleem Shahzad, Oliver Popov, Ibrahim Baggili (2016) A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis. Digital Investigation 16: S55-S64.
5. Sai Dasari Manendra, NRGK Prasad, Satish Dekka (2015) The Forensic Process Analysis of Mobile Device. Int J Comput Sci Inf Technol 6(5): 4847-4850.
6. O Connor, Rory V (2005) Software selection: towards an understanding of forensic software tool selection in industrial practice. International Journal of Technology Policy and Management 5(4): 311-329.
7. Horsman, Graeme (2018) I couldn't find it your honour, it mustn't be there!-Tool errors, tool limitations and user error in digital forensics. Science & Justice 58(6): 433-440.
8. Guo Yinghua, Jill Slay, Jason Beckett (2009) Validation and verification of computer forensic software tools-Searching Function. digital investigation 6: S12-S22.
9. Horsman Graeme (2019) Tool testing and reliability issues in the field of digital forensics. Digital Investigation 28: 163-175.
10. Talib Manar Abu (2016) Towards early software reliability prediction for computer forensic tools (case study). Springer Plus 5: 827.
11. Alvarez Paul (2004) Using extended file information (EXIF) file headers in digital evidence analysis. International Journal of Digital Evidence 2(3): 1-5.
12. Salama Usama et al. (2012) Metadata based forensic analysis of digital information in the web Annual Symposium on Information Assurance & Secure Knowledge Management 7.
13. Sun Xiaoting, Yezhou Li, Shaozhang Niu, Yanli Huang (2015) The detecting system of image forgeries with noise features and EXIF information. Journal of Systems Science and Complexity 28: 1164-1176.

14. Toevs Brian (2015) Processing of Metadata on Multimedia Using Exif Tool A Programming Approach in Python. Annual Global Online Conference on Information and Computer Technology (GOCICT) IEEE.
15. Beard Isaiah (2017) Digital Photos, Embedded Metadata, and Personal Privacy.
16. Lokhande PS, BB Meshram (2015) Digital forensics analysis for data theft.
17. Sanap Varsha Karbhari, Vanita Mane (2015) 8 Comparative Study and Simulation of Digital Forensic Tools. International Journal of Computer Applications 975: 8887.
18. Pallagani, Avinash, Garcia Mario, T David (2015) Implementation of a Prototype for Automated Event Sequence Reconstruction for Web Browsing data in Computer Forensics. Diss. Texas A&M University-Corpus Christi.
19. https://www.prodiscover.com/products-services
20. Mchatta Kharim Haji (2018) MSc Forensics Computing M08CDE: Master Individual Project Project Title: Forensics Tools and Data Hiding Techniques. Diss COVENTRY UNIVERSITY.
21. https://www.itnews.com.au/feature/review-prodiscover-incident-response-66292
22. https://accessdata.com/products-services/forensic-toolkit-ftk
23. https://www.scmagazine.com/review/accessdata-forensic-toolkit-ftk/
24. https://ericzimmerman.github.io/KapeDocs/#!index.md.
25. https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape.
26. https://www.sans.org/blog/triage-collection-and-timeline-generation-with-kape/
27. https://www.kroll.com/en/insights/publications/cyber/exploring-kapes-graphical-user-interface
28. Shala Lavdrim, Ahmet Shala (2016) File Formats-Characterization and Validation. IFAC-Papers OnLine 49(29): 253-258.
29. Nelson B, Phillips A, Steuart C, (2014) Guide to computer forensics and investigations. Cengage Learning.
30. https://exiftool.org/
31. Davis Naja (2007) Live memory acquisition for windows operating systems.
32. https://blog.eccouncil.org/an-introduction-to-computer-forensics-and-how-to-become-a-computer-hacking-forensic-investigator/
33. http://analogexif.sourceforge.net/help/
34. https://www.cyberstudents.org/blog-post/popular-forensic-software
35. https://resources.infosecinstitute.com/7-best-computer-forensics-tools/
36. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3